2005

Report of the

Auditor General of Canada

to the House of Commons

APRIL

Chapter 2

National Security in Canada—
The 2001 Anti-Terrorism Initiative:
Air Transportation Security, Marine Security,
and Emergency Preparedness

Office of the Auditor General of Canada

The April 2005 Report of the Auditor General of Canada comprises six chapters, and a Message From the Auditor General of Canada 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) 943-5485
E-mail: distribution@oag-bvg.gc.ca

Ce document est également publié en français.

Cat. No. FA1-2005/1-2E
ISBN 0-662-39693-6

Chapter

2

National Security in Canada—The 2001 Anti-Terrorism Initiative

Air Transportation Security, Marine Security, and Emergency Preparedness

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

Air Transportation Security, Marine Security, and Emergency Preparedness

Main Points

2.1 In December 2003—two years after it launched its anti-terrorism initiative—the government reorganized federal emergency planning, creating Public Safety and Emergency Preparedness Canada. The new department began an extensive reform program, but much remains to be done. Threat and risk analyses were not always used to guide the disbursement of funds by the previous agency to municipalities and provinces, resulting in poor allocation of funds. We found in a number of cases that programs do not appear to have achieved the intended results:

- In 2002 to 2004, federal funds were used to purchase equipment for first responders that did not have to be interoperable, losing a key opportunity to enhance the national capacity to respond to an emergency.
- The Office of Critical Infrastructure Protection and Emergency Preparedness, responsible for implementing a critical infrastructure protection initiative of Budget 2001, could not tell us what it had spent funds on. About one third of the funds allocated so far to this program may have lapsed.

2.2 Governance structures require continued attention. The government has established the Government Operations Centre to manage emergency responses, but the legislative and infrastructure frameworks remain uncompleted. Managing the budgets of projects that cut across several departments worked well in some cases, such as marine security and the CBRN Research and Technology Initiative, but failed in the cases of CBRN training for first responders and critical infrastructure protection. (CBRN refers to chemical, biological, radiological, or nuclear threats.)

2.3 The departments responsible for the CBRN Training Initiative estimated that about 6,000 first responders should be trained in how to intervene in and neutralize a serious event. We found that 200 people had been trained to this level so far under the CBRN Training Initiative.

2.4 Some key elements of the federal government's air transport security program are moving forward. The purchase and installation of explosives detection systems to screen passengers and baggage—an initiative by the Canadian Air Transport Security Authority (CATSA) at a cost of over $1 billion—are proceeding mostly as planned. Analyses of requirements and options were generally adequate.

2.5 Other elements, however, are working less well. Transport Canada told us it does not have a major problem with CATSA, but the Department has set no system-wide performance levels for CATSA and completed no assessments of its performance. The Department has not defined the sanctions it will use against CATSA if education and persuasion fail to get timely results.

2.6 Marine security programs have been based on an adequate threat and risk analysis. Implementing the Automated Identification System for ships encountered delays but is still expected to be completed by its original implementation date. The High Frequency Surface Wave Radar project, intended to provide continuous, real-time surveillance of Canada's coastal areas, represents an improvement in surveillance but will not provide full coverage. The government is acquiring fewer radar sets than considered necessary for complete coverage, and the radar will have a more limited range than originally forecast. The result will be gaps in coverage, with significant additional costs if full coverage is to be attained.

2.7 The government's implementation of the International Ship and Port Facility Security Code, necessary to keep Canadian ports and ships in the business of world trade, is generally going well. However, some certificates were issued on an interim basis, and security inspectors may be pressed to complete the inspections required for new certificates by the renewal deadline.

Background and other observations

2.8 This is the second of two audit reports on the federal government's anti-terrorism initiative announced in the 2001 Budget after the September 11 attacks on the United States. The government initially announced $7.7 billion for this initiative and subsequently added another $690 million.

2.9 Our first report, published in March 2004, addressed budget management, the allocation of funds, monitoring of expenditures, intelligence issues, and some aspects of air and border security. This chapter addresses air transportation security, elements of marine security, and emergency preparedness programs.

The departments and agencies have responded. In general, the organizations have agreed with our recommendations, although commitments toward remedial action remain vague in some cases. We found the response from Public Safety and Emergency Preparedness Canada to be positive, as the Department is already moving ahead in some areas.

Introduction

2.10 This chapter is the second of two on the government's Budget 2001 national security enhancement initiative. The first chapter was published in the March 2004 Report of the Auditor General of Canada (Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative). Excerpts from that chapter are provided as background in Exhibit 2.1

2.11 **Previous audit findings.** Our 2004 chapter addressed budget management, the allocation of funds, monitoring of expenditures, intelligence issues, and some aspects of air and border security. We reported the following:

- The government lacked a management framework to guide investment, management, and development decisions and allow it to direct complementary actions of separate agencies or choose among conflicting priorities.
- The government had failed to improve its security information systems to ensure that they could communicate with each other.
- We found a lack of co-ordination of intelligence and a failure to adequately assess the intelligence lessons learned from critical incidents such as the September 11 attacks.
- Lists used to screen visa applicants, refugee claimants, and travellers entering Canada had gaps and inconsistencies.
- Criminal intelligence data were not used in screening applicants for clearance to restricted areas at airports.

The government responded with actions to address our findings. We have not yet followed up on its response.

2.12 The Government of Canada released its first national security policy on 27 April 2004. The policy sets out an integrated approach to security issues across government to address a wide range of risks and threats. The government allocated an additional $690 million from the contingency reserves of Budget 2001 and Budget 2003 and provided new funding in Budget 2004. The policy focussed on three national security interests:

- protecting Canada and Canadians at home and abroad
- ensuring that Canada is not a base for threats to our allies
- contributing to international security

2.13 The policy sets out actions planned by the government in a number of key areas:

- intelligence
- emergency planning and management
- public health
- transport security
- border security
- international security

Exhibit 2.1 Federal response to September 11, 2001

Excerpts from March 2004 Report of the Auditor General, Chapter 3—National Security in Canada—The 2001 Anti-Terrorism Initiative

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**. 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 were the following:

- A new department, Public Safety and Emergency Preparedness Canada, was 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 co-ordinates integrated threat assessments, helps strengthen interagency co-operation, and assists 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 manages national security and intelligence issues and activities and government-wide responses to public health, national disasters, and security emergencies. It replaces the Ad Hoc Committee on Public Security and Anti-Terrorism.

* * * * *

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.

* * * * *

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.

Exhibit 2.1 Federal response to September 11, 2001 (continued)

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

2.14 Given the large number of programs and initiatives funded by the December 2001 Budget, we decided to examine air travel security, elements of marine security, and emergency preparedness in a second audit. This chapter reports the results of that audit.

2.15 The chapter focusses on three specific program areas funded from the 2001 Budget:

- **The integrity of the air transportation security system.** Transport Canada sets policy for and regulates the air transportation security system. We looked at how well it plays its role. We also looked at whether the implementation of explosives detection systems at Canada's airports was well planned and is proceeding smoothly. The 2001 Budget allocated more than $1 billion over five years for this purpose.
- **Marine security.** The 2001 Budget initiative identified marine security as a priority, but the government was unable to put forward a plan quickly. It formed the Interdepartmental Marine Security Working Group in 2001, which developed a multi-agency program. We audited two capital projects that were part of this initiative—High Frequency Surface Wave Radar and the Automatic Identification System for ships. We also audited the federal government's part in implementing the International Ship and Port Security Code, intended to secure Canadian ships and ports.
- **Emergency preparedness.** Budget 2001 allocated $513 million over five years to improve federal and national preparedness for chemical, biological, radiological, and nuclear attacks. We audited the accountability and management structure of the programs, the adequacy of the capacity being created, and the progress of training and exercise programs.

2.16 More details on the objectives, scope, approach, and criteria of the audit are included at the end of the chapter in **About the Audit**.

Observations and Recommendations

Air transport security

Security inspection and enforcement roles and responsibilities

2.17 Aviation security aims to protect the general public, passengers, crew members, airports, other aviation facilities, and aircraft against unlawful interference. Transport Canada has established a range of tools to promote security, including programs for prevention, detection, awareness, education, and deterrence. Security programs cover regulations that govern airport operators; air carriers; agencies that screen passengers and baggage before allowing them into the system; access to restricted areas; possession of weapons; persons under escort; and response to security threats. Transport Canada is responsible for enforcing its regulations. Its security inspectors can assess monetary penalties, remove a security screener's authority, and detain aircraft on the ground or recall an aircraft in flight should there be an immediate threat to security.

2.18 A second federal agency—the Canadian Air Transport Security Authority (CATSA)—plays a key role in security. Included in its responsibilities are the pre-boarding screening of passengers and the baggage and possessions they carry as well as the screening of airport workers entering restricted areas. CATSA can do this screening either directly or through a screening contractor. It is responsible for establishing the qualifications, training, and performance standards that security screeners must meet and for certifying that they meet them.

2.19 Many other organizations play a part in security. The RCMP and local police are responsible for law enforcement; local airport authorities are responsible for the physical security of airports; air carriers implement regulations intended to secure passengers, baggage, freight, and aircraft; cargo companies are responsible for the security of their operations.

2.20 Transport Canada is the policy-maker and regulator and, as such, occupies the lead role in air transport security.

2.21 The 2001 Budget allocated $2.2 billion over five years to strengthening aviation security. The most important measures taken by the government since September 11, 2001 include

- creating CATSA, through legislation, to take over passenger screening from the air carriers and also to screen non-passengers;
- deploying systems to detect explosives;
- providing airports with grants to improve airport security and policing;
- placing armed RCMP officers aboard some flights;
- improving aircraft cabin security;
- evaluating advanced technologies for airport security; and
- enhancing regulatory and oversight capacity.

Creating and operating CATSA accounted for $1.9 billion of the $2.2 billion allocated for aviation security. The remaining $300 million was to fund all other air security improvements.

Risk management has not been formalized

2.22 The Treasury Board Secretariat's Integrated Risk Management Framework calls risk management "a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues."

2.23 The Framework describes a process to identify issues, assess key risks, measure the likelihood and impact of risks and rank them accordingly, define the desired results, and select and implement strategies for managing or mitigating the risks (Exhibit 2.2).

2.24 Our objective in auditing aviation security was to determine whether Transport Canada's oversight of the air transport security system is adequate. We expected to find that the system was based on appropriate risk analysis and that Transport Canada was taking the necessary measures to ensure compliance with its security regulations.

2.25 We found that Transport Canada's approach to assessing security risks in air transport (to the extent that it has done so) is consistent with the

Exhibit 2.2 A common risk-management process

Source: Treasury Board Secretariat

Treasury Board Secretariat's Framework. However, it has not fully implemented formal risk management. At the time of our audit, one region of the Department was piloting a risk-based approach to managing the inspection process. Transport does have a general threat assessment that is updated annually by its intelligence directorate, which also sends specific notices and alerts to airports as needed. However, we did not find any comprehensive assessment of key risks or any measuring of the likelihood or potential impact of specific threats.

2.26 Transport Canada has done some work that partly meets the requirements of a sound risk management approach:

- An interdepartmental working group on aviation security was established in September 2003 to assess threats and determine appropriate action. However, its terms of reference limit it to assessing air carriers' applications for new overseas air routes. The working group has not been asked to develop an overall assessment of threats to aviation security.
- With the U.S. Transportation Security Administration, Transport Canada has assessed the potential impact of a specific threat as well as vulnerability to that threat, overall and at particular airports. This assessment met Treasury Board criteria but was limited to a single threat.
- Transport Canada relied on a series of teleconferences among senior security managers to deploy the additional security inspectors funded by the 2001 Budget and to supplement the existing minimum schedule of inspections. According to officials, they considered factors such as the size of airports, the number of flights, the riskiness of flight destinations, and the frequency of flights to the United States. While these decisions took into account the Department's experience and understanding of intelligence information, they were not documented as a formal risk analysis.

We also noted that the RCMP uses formal risk assessment in deploying its Aircraft Protective Officers aboard flights, except where carrying an officer is mandatory.

2.27 The assignment of inspection resources appears to be weighted toward risks from passengers and baggage. Risks from air cargo and general aviation (that is, small private and chartered aircraft) attract less scrutiny, despite the level of concern they have generated. Transport officials pointed out that they had doubled the number of cargo inspections and had implemented new programs of cargo security awareness with industry. Nevertheless, it is not clear to us that inspection resources and assignment of tasks have been allocated appropriately. Nor is it clear how funding for security inspection was allocated between major airports and smaller ones, when both are gateways to the entire system. Because the inspection program has not been based on a documented risk analysis, we could not conclude whether the number of inspectors and the frequency of inspections are appropriate.

2.28 Transport Canada officials told us that they had not done a wider analysis before allocating the 2001 Budget funding for inspection, because the federal government had emphasized passengers as the key risk and the Budget had directed funding only to passenger transportation. The officials told us they intend to begin a complete review of security for all modes of transportation in 2005 in order to develop a security strategy.

2.29 **Recommendation.** Transport Canada should complete a formal analysis of threats and risks to the entire air transport system and use the results as a basis for deploying resources and focussing enforcement efforts.

Transport Canada's response. Transport Canada recognizes the importance of risk management, which has been an essential foundation of its aviation security program since its inception in the 1970s. More recently, the Department has initiated a comprehensive Transportation Security Strategy, which will examine risk in all modes and activities within each mode. The strategy will include a formal threat-and-risk-analysis instrument that could be used in risk management decision making for regulatory, legislative, and enforcement activities (spring 2006). In the interim, Transport Canada will continue to rely on its inspectors and existing analytical capacity to address emerging security needs.

The security inspection program has been expanded

2.30 We reviewed how the security inspection system operates. We interviewed senior Transport security managers at five major airports and at national headquarters about the staffing of security inspection positions, training of security inspectors, and local ability to implement the inspection cycle called for by Transport policy. We reviewed organization charts and staffing plans for the airports we visited. We also reviewed headquarters' quality control program for security inspection.

2.31 Our review did not identify any major difficulty in local capacities to carry out the number of inspections required by headquarters. Positions were nearly all filled, and managers did not report any difficulty recruiting and retaining inspectors. Managers said the training program was good, a major improvement over the previous one.

2.32 We noted that the annual Comprehensive Security Review called for by headquarters since April 2004 had not yet been carried out. Transport officials said that several comprehensive reviews were conducted in 2001, one just after the September 11 attacks. Officials were concentrating on expanding the inspection service in 2004–05. The new inspection policy will come into effect fully in 2005–06.

2.33 Transport Canada established a three-person Quality Review division in February 2003 but we found that it had not yet done any quality reviews, though officials told us that in 2004–05 they were intending to complete two quality reviews in Toronto and Montréal. Failure to conduct a quality review of security inspections carries a risk that standards will not be enforced uniformly, with poor inspection quality as a result. Our review of inspection

files in the airports we visited found several inspections that had never been properly documented and for which there was no evidence of completion.

Problems in enforcing corrective action

2.34 Transport Canada's security inspection system is the primary means for security managers to know whether the security system is meeting the regulated standards. We therefore assessed the Department's ability to analyze breaches of security and enforce corrective action when systemic problems become evident.

2.35 **Analysis of security breaches.** We assessed the quality of the data in the main inspection database (called SEMIS) to determine whether we could rely on it in our audit. We examined 110 files selected judgmentally at the five airports we visited. We also asked the senior Transport Canada security manager at each airport to comment on the accuracy of summary statistics generated by the SEMIS system.

2.36 We found that SEMIS data were completely accurate in only 60 percent of the files we reviewed. The most common error was misstating whether the investigation had been closed or not. Transport security managers at the airports we visited did not regard SEMIS as accurate, so they maintained their own local databases and files.

2.37 Transport Canada managers at headquarters acknowledged that the SEMIS database contained errors. Headquarters managers said they intend to clean it up but have not been allocated funds to do it.

2.38 Given the problems with SEMIS, Transport Canada replaced it in April 2004 with a new system called SEPIRS. The new system is intended to address the shortcomings of the old system, but data from before 2004 require validation to determine the extent of their inaccuracy.

2.39 We also asked Transport Canada security managers how they assessed risks and identified trends in non-compliance. At most locations, they use data from their own databases and perform their own analysis. Several complained that they had no access to data from other regions and therefore could not identify trends by specific carriers who operate nationally. Their main means of assessing trends in risks and non-compliance are the weekly conference calls by the senior security managers across the country and the monthly reports prepared by the Quality Review division.

2.40 The lack of an accurate central database has hampered Transport Canada's ability to assess emerging trends. Officials told us that the new SEPIRS system will allow monthly reports to be seen by all the regions.

2.41 **Problems in enforcement.** A security system must be able to not only recognize risk and non-compliance but also enforce timely corrective action. We therefore looked for issues that affected the overall performance of the enforcement system.

2.42 Security of passenger air travel is based on a number of security measures that include the gathering of intelligence, law enforcement by

police, questioning by ticket agents, primary screening of passengers, secondary screening of some passengers, use of protective officers on some flights, and fortification of the flight decks of aircraft.

2.43 Transport Canada has not analyzed the overall effectiveness of its security systems; it has only one security performance measure in place: the "infiltration failure rate" of passenger screening. This is the rate at which screeners fail to detect "threat objects" such as a simulated knife, simulated gun, or simulated explosive device when the inspectors try to carry them through passengers screening. However, the Department has chosen to classify that measure and the related information; accordingly, we may not report it.

2.44 When Transport Canada's inspectors encounter a failure in CATSA's procedures, including an infiltration failure, an enforcement letter is issued to CATSA. Transport Canada has issued such letters to CATSA for failures to meet security standards. Examples include

- incidents where unauthorized persons gained access to secure areas;
- cases where there were failures to detect unauthorized objects with metal detectors;
- instances where employees did not keep adequate logs, communicated ineffectively, performed poorly, or lacked valid certifications or designations; and
- cases where screeners failed to conduct random tests properly. Transport Canada later issued an exemption to its regulations to recognize the difficulty of complying with the requirement for random testing while improving the screening process at the same time.

2.45 In Transport Canada's inspections of CATSA that were unrelated to infiltration tests, only three to four percent identified a deficiency that resulted in an enforcement letter. CATSA officials told us they considered some of those deficiencies to be minor. However, Transport Canada does not categorize its enforcement letters by importance.

2.46 Neither Transport Canada nor CATSA adequately tracked action taken in response to individual enforcement letters. Neither organization had a complete and accurate inventory, and the numbers of letters on file at Transport, CATSA, and in the Transport database did not agree. Neither agency could find responses to all the enforcement letters. We could not find responses to about 12 percent of enforcement letters related to infiltration tests and to 16 percent of letters addressing other deficiencies. CATSA officials did point out that they had changed procedures significantly in response to inspection results. During the audit, CATSA also began to track enforcement letters and its responses to them more closely.

2.47 Aspects of Transport Canada's enforcement model seem unsuited to dealing with a government agency that, like CATSA, is the sole provider of a security service. An air carrier or airport authority that showed persistent non-compliance would eventually be fined. However, Transport officials did not think monetary penalties against CATSA would be appropriate since, in

their view, fines would inevitably redirect resources away from the delivery of CATSA's mandate. Further, because fines for security breaches are not disclosed, the officials felt that monetary penalties would have a limited impact on CATSA.

2.48 Transport officials told us they do not have a major problem with CATSA. Nevertheless, we found the following:

- Transport Canada has never established any system-wide performance standards for CATSA that would rate as satisfactory anything less than 100 percent compliance.
- Transport security officials expressed dissatisfaction with CATSA's performance in specific cases and have threatened to fine the agency.
- Transport Canada has never completed an assessment of CATSA's overall performance to determine whether additional enforcement measures are required.
- Transport staff were not aware of trends or patterns in the effects of enforcement actions.

2.49 We do not believe that Transport Canada's enforcement regime works well in the case of CATSA. No performance goals have been established. The Department's internal studies and analyses are not adequate, and there appear to be no effective sanctions available should education and encouragement fail.

2.50 **Recommendation.** Transport Canada should put in place system-wide performance measures that specify what it considers to be satisfactory performance by the Canadian Air Transport Security Authority (CATSA).

Transport Canada's response. Transport Canada has developed a comprehensive enforcement program, including monitoring and inspection, to ensure compliance with the rules. With respect to CATSA, Transport Canada has taken, and will continue to take, an incremental approach to enforcement. While Transport Canada does not consider monetary penalties to be necessarily the best compliance tool, it can take appropriate enforcement action, drawing if necessary on the range of legislative and administrative mechanisms available, including holding directors and officers accountable. In addition, Transport Canada is now developing system-wide qualitative and quantitative measures of performance by screeners and equipment, which will be reviewed on a regular basis. Measures will be finalized by early 2006.

Installation of explosives detection systems is going well

2.51 The 2001 Budget allocated over $1 billion to purchase, deploy, and operate advanced explosives detection systems (EDS) at airports across the country. These systems are to be in place before 1 January 2006.

2.52 Pre-boarding screening of passengers and the effects they will carry on board includes physical searches and machines that can detect minute traces of explosives residue.

2.53 "Hold-bag" screening is the security screening of luggage that passengers have checked to be stowed in the hold (cargo compartment) of the plane. Screening officers identify threat objects by using enhanced X-ray or CAT-scan machines and other explosives trace equipment or by physically searching the bag.

2.54 Part of CATSA's screening responsibility includes acquiring, installing, and maintaining explosives detection equipment at airports and ensuring compliance with the regulations and standards Transport Canada has established for EDS. Transport Canada monitors operations and equipment for passenger and hold-bag screening to ensure that the systems meet its standards.

2.55 Our audit looked at whether Transport Canada and CATSA each managed its part adequately in acquiring and implementing explosives detection systems. We reviewed five Class I airports (Vancouver, Montreal, Calgary, Ottawa, and the new Terminal 1 in Toronto); two Class II airports (Saskatoon and St. John's); and two Class "other" airports (Sydney and Lethbridge).

2.56 CATSA was to equip 89 airports across Canada for hold-baggage screening. It defined projects in these 89 airports and had completed about half of them at the time of our audit. CATSA reviewed the proposals from airports against its guidelines, proposed alternative solutions, and reached agreement with the airports on the installation of EDS. The airports were responsible for project construction and for installing the systems, and CATSA reimbursed them for their approved costs. We observed that project objectives were clearly defined, project implementation reports were given to CATSA's Board of Directors, and there was an information system to track whether projects were on schedule and to track the costs.

2.57 CATSA's capital budget was based on completing the defined projects but did not include EDS at the domestic portion of a major airport, which would be undergoing renovations first. Transport Canada told us that to protect vulnerabilities in the meantime, it will ensure a level of security equivalent to that in the rest of the transportation system. Proceeding in this way appears to be reasonable, avoiding the expense of putting new systems in place that would have to be removed during renovations and then reinstalled. However, the size of the financial obligation this approach creates for CATSA is not clear.

2.58 We expected that Transport Canada would have adequately defined the need for the EDS project and analyzed options. We found that it had identified the need for new EDS machines and considered EDS approaches, had done some of the research, and had analyzed options and chosen equipment well before September 11, 2001. It completed another options analysis after September 11.

2.59 We noted a lack of life-cycle-costing information and analysis by Transport Canada, and CATSA only recently began to analyze the costs of explosives detection equipment over its life cycle. While the choice of

equipment was therefore based on incomplete information, we believe that given the emergency, the decisions were reasonable.

Marine security

2.60 At the time of the 2001 Budget, the government did not know exactly which aspects of marine security needed to be addressed and in what order of priority. As an immediate response, the Budget 2001 initiative identified a few "quick fix" improvements such as increased aerial surveillance of Canada's maritime zone. An initial investment of $60 million was allocated to marine security in the knowledge that a more comprehensive approach would be needed.

2.61 After about $25 million of this amount had been allocated to specific projects, an Interdepartmental Marine Security Working Group of senior officials conducted threat assessments, developed options, and made recommendations to ministers. The government responded by allocating an additional $172.5 million to fund improvements in marine security from 2003 to 2008.

2.62 This new funding is designed to improve

- awareness of what is happening in Canada's coastal waters (surveillance or domain awareness);
- security of port facilities and waterways;
- response time to events that threaten security; and
- rates of inspection of vessels, ports, and cargo containers.

2.63 Furthermore, the International Maritime Organization (IMO) developed international standards for the security of ships and port facilities. As a signatory to conventions under the IMO treaty, Canada became responsible for implementing the Automated Identification System (to identify vessels) and the International Ship and Port Facility Security Code. Our audit looked at the implementation of those two projects and a third, the High Frequency Surface Wave Radar installation.

Automatic Identification System for ships is being implemented

2.64 The International Maritime Organization requires that all ships of a certain size be fitted with an automatic identification system (AIS) that has transponders similar to those on aircraft. An AIS transponder broadcasts a message that identifies the vessel, its heading, and its speed. This continuous broadcast can be received by vessels, shore stations, or aircraft outfitted with AIS receivers. The completion of the Canadian Coast Guard's AIS shore-based receivers is expected to enhance Canada's ability to identify and track AIS-equipped vessels in its coastal areas.

2.65 The Canadian Coast Guard is installing equipment on shore to allow the tracking of AIS-equipped vessels up to 40 nautical miles from shore, at an estimated cost of $27.5 million over five years. The St. Lawrence Seaway Management Corporation has already implemented this system in the St. Lawrence River.

2.66 We have two observations. First, a threat and risk analysis by the marine security Working Group identified four priority areas, but the allocated funding was enough for only the top three; we did not see a plan for addressing the shortfall. Second, setting up a project management IT system and obtaining funding approvals encountered delays, but the Coast Guard intends to complete the project by its original implementation date.

2.67 Canada is a signatory to the International Convention for the Safety of Life at Sea (SOLAS); the new International Ship and Port Facility Security Code (ISPS); and amendments to both, adopted in December 2002 at the Diplomatic Conference of the International Marine Organization. Canada was required to implement, by 1 July 2004, the domestic ship and marine facility security requirements stipulated in the ISPS Code.

2.68 Transport Canada's implementation of the ISPS Code was achieved by incorporating it in the Marine Transportation Security Regulations under the *Marine Transportation Security Act.*

2.69 The Code and the Regulations apply to commercial vessels that weigh 500 tons (gross tonnage) or more and to marine facilities and ports that serve such vessels. Regulations require that these vessels and facilities complete security assessments and security plans and designate security officers.

2.70 Because Canada wants to harmonize its marine transportation regulations with those of the United States, it extended its regulations beyond the IMO requirements to also cover

- cargo vessels of 100 tons (gross tonnage) or more;
- vessels that tow barges carrying certain dangerous cargoes;
- vessels carrying more than 12 passengers; and
- marine facilities and ports that serve these vessels.

2.71 We expected Transport Canada to ensure that the design of the national framework for implementing the ISPS Code in Canada would comply with international requirements. We further expected it to ensure that Canadian ship owners and port facility operators would implement the national framework to meet international requirements and the regulations under the *Marine Transportation Security Act*.

2.72 We found that Transport Canada's regional offices and marine inspection officers maintained good relations with ships and port facility operators during the process of issuing a security certificate. Where security plans required additional preparation or the formal appointment of a ship or port facility security officer, interim security certificates were issued. Future demand for renewals of security certificates could place considerable pressure on Transport Canada's marine security inspectors to complete the required inspections before the renewal deadline.

2.73 The ISPS Code includes standards to classify and increase security levels in response to threats, as well as procedures to be followed until information becomes available that justifies a return to lower levels. We found that the criteria used by Transport Canada to increase marine security levels are not defined clearly.

2.74 Overall, Transport Canada successfully completed the necessary procedures for issuing security certificates to all ship and port facility operators required to have them, and it met the ISPS Code Agreement deadline of 1 July 2004.

High Frequency Surface Wave Radar faces funding and regulatory problems

2.75 On the basis of its threat and risk analysis, the marine security Working Group supported the development of High Frequency Surface Wave Radar (HFSWR) that, as a long-range, over-the-horizon radar, can provide real-time, continuous radar surveillance extending up to 200 nautical miles.

2.76 National Defence has worked for 15 years on a research project to develop radar effective over water to a distance of 200 nautical miles. The readiness trial was completed in August 2004, and the Department has informed us that system-acceptance tests were completed recently. The results, while promising, have not yet been analyzed completely.

2.77 We examined this initiative as a capital project, assessing the

- needs definition,
- options analysis, and
- project management and definition.

2.78 We note two concerns about the ongoing development of the HFSWR project:

- A National Defence study indicates that full coverage would cost a total of $220 million rather than the $43.1 million the Department was allocated. National Defence recommended acquiring and installing equipment at only four to six sites. Research has shown that HFSWR does perform to expectations during normal circumstances, but it does not operate to its full range under certain conditions such as at night, during meteorological disturbances, and in heavy seas. Increased costs and reduced capability leave major gaps in the coverage of Canada's coastlines. However, National Defence believes that this radar provides additional information not available from existing surveillance systems. We were unable to obtain evidence that explains how gaps in coverage would be closed, the cost of closing them by other means, or the security implications of leaving them unaddressed.
- National Defence has not yet obtained a permanent licence from Industry Canada to operate the system. A permanent licence can be issued only after Industry Canada is assured that the system will not interfere with the operations of other licensed users of the same radio-frequency band.

Federal emergency preparedness

2.79 The front line of defence in a terrorist attack is the first responders—the police officers, firefighters, emergency medical care providers, and emergency management officials who make up specially trained hazardous materials teams, urban search and rescue units, bomb squads, and tactical units. Most of them work for a provincial, territorial, or municipal government.

2.80 The National Security Policy of April 2004 says that first responders are at the heart of the emergency management system; the federal government "will often play only a supporting role in emergency management to provinces and territories, communities and the private sector." The Policy identified the need to modernize the national system of emergency management.

2.81 On September 11, 2001, Canada's approach to emergencies was based on a Cold War approach. The system was based on a highly decentralized and distributed division of responsibilities among front line responders, provinces and territories, and lead departments at the federal level. Although the 2001 Budget had allocated significant additional funds to improving emergency preparedness, by 2003 the government recognized that organizational improvements in this area would be needed to make the desired progress. It therefore removed the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) from National Defence and merged it with the Solicitor General and the National Crime Prevention Centre to form Public Safety and Emergency Preparedness Canada (PSEPC).This new department is intended to improve the integration of government efforts across the public safety program, linking the various federal programs together more closely.

2.82 In its first year of operation, PSEPC initiated a major legislative program to give substance to the government's goal of "a seamless national emergency management system." The Department has also launched the Government Operations Centre, begun the development of the National Emergency Response System (NERS), and improved the readiness and exercise program. We report here on the progress made and work still to be done below. Many of the gaps and implementation problems our audit found originated in the program before the new department was established.

2.83 The 2001 Budget allocated $513 million over five years to federal and national efforts to prepare for chemical, biological, radiological, and nuclear threats, or CBRN (Exhibit 2.3). The funds were to enhance existing laboratory networks so they could more quickly detect and identify biochemical threats. The government also decided to buy new protective equipment for emergency response teams and improve their training.

2.84 In this audit, we looked at whether federal programs to enhance emergency preparedness for a CBRN event have been managed adequately. We also looked at critical infrastructure protection. Budget 2001 had allocated $396 million to enhancing the management of critical infrastructure protection. We looked at whether threat and risk assessments had been used to prioritize investments in infrastructure and at the progress achieved to date.

2.85 We did not examine progress made by provincial, territorial, or municipal governments. Our findings relate solely to the federal government.

Exhibit 2.3 Chemical, biological, radiological, and nuclear events

The federal government has recognized that Canada is not immune from the threat of terrorism following September 11, 2001, and there is growing concern over the threat of chemical, biological, radiological, or nuclear (CBRN) terrorism.

Potential CBRN weapons encompass a range of agents:

- biological (such as smallpox and anthrax)
- chemical (such as sarin gas disseminated by explosives or aerosols)
- radiological/nuclear (such as radioactive material scattered by conventional explosives)

As with other types of emergencies, responsibility for CBRN-incident response is shared by federal, provincial, and municipal governments. Civil emergencies are initially dealt with by first responders—police, firefighters, and emergency medical personnel. If additional assistance is required, local officials contact the province or territory, who in turn can seek assistance from the federal government.

Source: Government of Canada, February 2003

2.86 To examine emergency preparedness for a CBRN incident, we looked at three areas:

- chain of command—that is, who is in charge of the response to an incident;
- federal and national capacity to respond to an incident (national capacity being the combined resources of federal, provincial/territorial, and municipal agencies); and
- the testing and exercising of response plans.

The chain of command remains complex

2.87 We expected to find a clearly established chain of command to guide the federal response to a CBRN incident. This would mean that federal roles and responsibilities would be clearly defined and would link consistently with response plans of provinces and territories.

2.88 Canada's approach to managing emergencies has been based on a division of responsibilities among first-line responders at the municipal and provincial/territorial levels and the lead departments at the federal level.

2.89 The National Security Policy stated the problem clearly:

> National emergency co-ordination currently suffers both from the absence of an effective federal-provincial-territorial governance regime and from the absence of commonly agreed standards and priorities for the national emergency management system.

The government is taking steps to rectify these issues, but we found that they go only partway to establishing a clear command and control structure.

2.90 Before December 2003, the nature of an emergency determined which federal department had the lead role in managing the response. Health Canada would manage a biological, radiological, or nuclear emergency and Transport Canada the cleanup of a transportation accident involving biological, chemical, or radiological materials. Natural disasters would be managed by the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) and incidents affecting the food chain by the Canadian Food inspection Agency. If any of these incidents proved to be an act of terrorism, leadership would immediately shift to the Department of the Solicitor General.

2.91 December 2003 was when, as already noted, OCIPEP was moved out of National Defence and merged with the Department of the Solicitor General to create Public Safety and Emergency Preparedness Canada (PSEPC).

2.92 As part of creating PSEPC, the government put forward legislation (Bill C-6) that would provide for the leadership role of the Minister of Public Safety in the event of a national emergency. The Minister would be responsible for providing strategic co-ordination while respecting the Prime Minister's prerogative in matters relating to national security and the statutory authorities of other ministers. According to officials, however, Bill C-6 does not provide the specific powers needed to activate this role. Those powers are expected to be contained in revisions to the *Emergency Preparedness Act* on which PSEPC plans to begin consultations in the spring of 2005.

2.93 **Recommendation.** Public Safety and Emergency Preparedness Canada should finish drafting the revisions to the *Emergency Preparedness Act* as soon as possible to finalize the definition of the minister's powers and responsibilities.

Public Safety and Emergency Preparedness Canada's response. The modernization of the *Emergency Preparedness Act* is a commitment under the National Security Policy. A discussion paper has been drafted outlining the proposed powers and authorities of the Minister of Public Safety and Emergency Preparedness. The paper reflects the emerging requirements of emergency management. Consultations with stakeholders will begin in spring 2005.

2.94 **A new national response system**. PSEPC is developing a new national emergency response system (NERS) aimed at eliminating overlap and duplication in the crisis- and consequence-management stages of response (Exhibit 2.4). It intends to standardize all federal response plans and their links to provincial plans, but it has not committed to a completion date. We were told that the National Counter-Terrorism Plan and the National Support Plan will be revised and become part of the NERS, but currently the NERS is not in a form that could replace an existing federal plan.

Exhibit 2.4 National Emergency Response System (NERS)

NERS is an "all hazards" response structure designed to co-ordinate the federal response to emergencies of national importance, including support to provinces, territories, and the federal departments involved. It will provide for national policy direction and strategic co-ordination.

A national response within NERS may also include issuing a notification, a warning, and/or an alert to the public.

NERS will not change existing departmental mandates but rather will co-ordinate mandates in a harmonized federal response.

NERS is based on functionally oriented groups staffed by personnel from Public Safety and Emergency Preparedness Canada and other federal departments. The response structure can be activated partially or fully, using escalating levels of operations that correspond to emerging, imminent, or occurring emergencies. Each response level represents an increase in the federal capability and capacity to respond.

Source: Public Safety and Emergency Preparedness Canada

2.95 PSEPC has conducted extensive consultation on the NERS within the federal government and with the provinces and territories. We were told that the government has approved the approach in principle. Officials have also told us that they are developing the new system's structure and hope to get formal Cabinet approval sometime in spring 2005. In our opinion, if NERS is to work it must have official sanction and, equally important, support from all federal agencies involved in responding to a national emergency—which, by nature, can involve several agencies. Until the government fully implements the NERS, elements of the federal response will still be managed by individual departments.

2.96 **Recommendation.** Public Safety and Emergency Preparedness Canada should work with the other federal agencies to clarify the command and control structure governing the federal response to emergencies.

Public Safety and Emergency Preparedness Canada's response. Leadership will be exercised through the command and control structure of the National Emergency Response System (NERS). In addition, changes to the *Emergency Preparedness Act* will reinforce the authority of the Minister of Public Safety and Emergency Preparedness to co-ordinate the actions of all federal players in emergencies of national significance.

2.97 **Recommendation**. Public Safety And Emergency Preparedness Canada should obtain its federal partners' formal agreement to the National Emergency Response System as soon as possible.

Public Safety and Emergency Preparedness Canada's response. We agree with the recommendation. A formal agreement to adopt the National Emergency Response System (NERS) will be sought with federal partners. There will be a good opportunity to validate the NERS through Exercise Triple Play in April 2005. In addition, provincial and territorial partners have agreed with the approach taken by the federal government.

2.98 **Co-ordinating operations centres**. We identified 27 operations centers in departments across the federal government whose operating capacities and technologies vary. We noted a lack of integration among these centres. In September 2001, OCIPEP did not have secure communications with these federal operations centres or with those of Canada's allies.

2.99 The National Security Policy of April 2004 announced the creation of a new Government Operations Centre in Public Safety and Emergency Preparedness Canada (PSEPC) to manage the federal response to emergencies. As of September 2004, the Centre has secure communications with other federal operations centres and with the United States and the United Kingdom. Co-ordination between individual departments' operations centres and the Government Operations Centre is an important element of the NERS.

2.100 The Centre's basic monitoring activities began in September 2004, but its emergency response capacity has not been validated in an exercise. It does not have command and control authority over the federal response when the lead resides in another federal department. In anticipation of the legislative changes, PSEPC officials are developing criteria for use of the Centre by other government departments as well as guidelines for transferring the federal lead to PSEPC when that is considered to be in the national interest. We note that the Government Operations Centre (GOC) is a critical component of the NERS concept of operations, which calls for the GOC to be proactive in conditions of emergency or uncertainty. Each of the response levels provides additional resources to ensure that the GOC has the capability and capacity to co-ordinate timely readiness and response activities. In practical terms, as the response level increases, the staffing and resource levels of the various functional groups will also increase.

Integrated plans are essential to an effective response

2.101 Another important element of the NERS is the link between national and departmental emergency plans.

2.102 Managing the federal response to a CBRN event could draw on a number of emergency plans. For example, we reviewed the following:

- National Counter-Terrorism Plan
- National Support Plan
- Federal Nuclear Emergency Plan
- Food and Agriculture Emergency Response System

2.103 We found that departmental plans are vague on how they would link together to form a co-ordinated federal response. Section 7 of the *Emergency Preparedness Act* requires that departments prepare emergency response plans for areas within their mandates. We noted a potential, as emergencies develop and implicate more departments and agencies, for conflict between having to work together with other departments and supporting the line responsibilities of their own mandates. Officials at PSEPC could not show us an inventory of departmental emergency response plans that could be activated in the event of a CBRN terrorist event. Nor could they provide us with an analysis

showing how, in a complex emergency involving several departments, the plans would work together to achieve a seamless federal response.

2.104 To achieve a national response, federal response programs need to be integrated not only across departments but also with those of other jurisdictions. We expected to find that federal response plans would link across jurisdictions consistently. However, we found the National Counter-Terrorism Plan and the National Support Plan to be inconsistent in the level of detail and the depth to which they link with response plans of the provinces.

2.105 **Recommendation.** Public Safety and Emergency Preparedness Canada should work with its federal partners and the provinces and territories to improve the co-ordination of response plans.

Public Safety and Emergency Preparedness Canada's response. We agree with the recommendation. Work has started on improving the co-ordination of response plans with provinces and territories. This initiative is also one of the action items flowing from the Federal-Provincial-Territorial Ministerial Meeting on Emergency Management, held on 24 January 2005.

Building capacity to respond to terrorist events

2.106 To improve the national capacity to respond to CBRN events, the federal government chose two areas of action: enhancing the capacity of federal agencies to respond, and increasing the capacity of provincial and municipal first responders.

2.107 The $513 million that Budget 2001 provided to enhance CBRN equipment and response capacity was allocated to a number of federal departments. The CBRN Research and Technology Initiative was created to distribute some of the funding and to allocate research and development projects. The RCMP, Canadian Forces, Health Canada, and Transport Canada were specifically tasked with developing a CBRN response capability.

2.108 Risk management principles acknowledge that although risk cannot be eliminated, enhancing protection from existing or potential threats can help reduce it. Accordingly, a risk management approach is a systematic process to analyze threats, vulnerabilities, and the criticality (or relative importance) of assets to better support key decisions.

2.109 We expected to see that programs designed to enhance capacity had been based on risk analyses and scenarios setting out what could happen, how departments should respond, and what resources the responses would require. Threat and risk assessments are key tools to determine where and how to establish programs.

2.110 **The RCMP is increasing capacity.** The RCMP was allocated $23 million over five years to equip and train first responders in its force and to develop specialized response teams. We found that it prioritized its capacity investments according to threat and risk analysis.

2.111 The RCMP developed a CBRN doctrine and concept of operations as a basis for its equipment purchases and training. It has now equipped and

trained 3,600 members to a basic response level and is scheduled to equip and train all 15,000 members of its regular force by April 2006. CBRN response training is now included in its training curriculum and, effective October 2004, all new graduates have received this training.

2.112 The RCMP has also equipped and trained four specialized two-member CBRN emergency response teams that support local first responders. Its plan to equip and train such teams was based on threat and risk assessments. The original assessment of the need for a national response capacity determined that eight teams of six to eight members each were needed. However, we were told that funding was provided only for a smaller response capacity.

2.113 The teams are equipped with CBRN-capable bomb suits; protective suits; detection, mitigation, and neutralization devices; and the capability to conduct forensic scene examinations in a CBRN environment. However, the small number and size of the teams and the large geographic areas to be covered could significantly delay the response in some regions. The RCMP has not yet determined how it will meet the identified need.

2.114 **Recommendation.** The RCMP should improve its capacity to respond to chemical, biological, radiological, and nuclear emergencies.

RCMP's response. The RCMP originally estimated the need for highly specialized CBRN response teams to be deployed regionally across Canada to supplement other response capacities. At the same time, the RCMP identified various other CBRN response requirements.

Since that time, we have made extensive progress toward training and equipping all RCMP members as CBRN first responders, able to assess and undertake primary containment of possible CBRN incidents.

The specialized Regional Response Teams are located in the Pacific, North West, Central, and Atlantic regions. They operate in conjunction with front-line responders and the Joint National RCMP/DND CBRN Response Team to provide a measured response in all parts of Canada.

The RCMP will assess the optimum size of the Regional Response Teams, taking into account current levels of training, including with partner agencies, as well as integration, new technologies, and availability of resources.

2.115 **National Defence has a limited role.** In 2002, the National CBRN Response Team was established, combining the resources of three federal departments. The RCMP has the overall lead and handles CBRN explosive ordinance and forensic evidence. The Public Health Agency of Canada (PHAC, created in September 2004 to assume some of Health Canada's responsibilities) provides emergency medical teams and a transportable lab to deal with biological hazards. National Defence provides its Joint Nuclear, Biological and Chemical Defence Company, whose primary mission is to support the RCMP, the first-responder community, and civil authorities with a dedicated military capability to respond to CBRN terrorist activities. Exhibit 2.5 provides more detail on the role of the Canadian Forces.

Exhibit 2.5 The Role of the Canadian Forces

While the entire Canadian Forces is potentially available to provide support, its primary role is not that of a first responder. The Forces can provide general support to provinces and territories to deal with the consequences of a chemical, biological, radiological, or nuclear event at their request but are not specifically tasked with this role. In December 2003, the government announced "an increase in the Canadian Forces Reserves available for civil preparedness, including a capacity to deal with natural disasters and local emergencies." The Reserves are not currently equipped and trained for this capacity, but National Defence is studying the feasibility of using them.

Source: National Defence

2.116 Budget 2001 allocated $30 million to National Defence to establish a new military unit, the Joint Nuclear, Biological and Chemical Defence Company. This military company can be used to support other government departments and the provinces and territories in their responses to a CBRN terrorist event. An evaluation by National Defence found "serious command and control issues" with the new unit.

2.117 **Emergency medical teams have not been created.** In December 2001, Health Canada was allocated $501,000 to develop Health Emergency Response Teams—rapid response teams of physicians, nurses, and medical technicians. During emergencies, these federally trained medical teams are to come to the support of local health care workers. A national office was established and given a broad mandate to oversee funding, recruitment, equipping, and deployment of the teams. In January 2003, Health Canada was allocated $626,000 annually to train health care workers in the prevention and treatment of smallpox. As part of this funding, the Department was to train provincial Smallpox Emergency Teams to immunize the public in the event of a smallpox epidemic. At the time of our audit, neither Health Emergency Response Teams nor the Smallpox Emergency Teams had been established. In both cases, officials from Health Canada now with PHAC told us that there are legal issues that have yet to be resolved.

2.118 Health Canada and the Public Health Agency of Canada are mandated to support the provinces and territories in managing the public health aspects of an emergency. A Budget 2001 allocation of $88.6 million over five years is targeted to strengthening their public security and anti-terrorism response capacity. We expected that investments would be prioritized on the basis of risk assessments and casualty scenarios, but we found limited use of such analyses.

2.119 PHAC manages the National Emergency Stockpile System (NESS) previously managed by Health Canada. The NESS is a cache of medical equipment and pharmaceuticals contained in warehouses across the country and ready to be sent to provinces and territories at their request. Budget 2001 allocated $7.9 million to replenishing this stockpile. We expected that the contents would be based on a risk assessment and that plans would be in place to ensure timely, efficient distribution.

2.120 It is not clear what role the stockpile plays in the emergency management system. Neither its objectives nor its contents are managed under a federal emergency response plan. The contents of the stockpile are not based on a risk assessment. The stockpile contains no CBRN equipment, such as protective gear, detectors, and decontamination showers and apparatus. It does contain a quantity of CBRN pharmaceuticals and medical countermeasures.

2.121 During our audit, PHAC completed the first stage of a strategic analysis examining the role of the National Emergency Stockpile System.

2.122 **Transportation issues**. A study looking at emergency transportation issues concluded that existing transportation arrangements for the NESS are "moderately reliable." Parts of the national emergency stockpile were moved after September 11, 2001 to allow for their distribution anywhere within 24 hours. Previously, the transportation and distribution of supplies in an emergency had been problematic and arranged on an ad hoc basis. For example, in response to the grounding of so many civilian aircraft on September 11, provincial officials requested supplies from the NESS. The only viable option for moving them was a military airlift. The plan was to load transport trucks with beds and blankets and send them to the Ottawa airport. Late on the night of September 11, it became clear that the trucks would have to be sent instead to CFB Trenton, because the Canadian Forces no longer kept equipment at Ottawa to load aircraft. A departmental after-action report concluded that these logistical problems resulted in a significant delay in shipping some of the supplies. Our view is that in an emergency, time can be a critical factor and it is not a good point at which to develop alternative distribution arrangements.

2.123 We recognize that the complexity of moving NESS supplies efficiently in an emergency is affected by the distances involved, the mode of transport, and the need for specialized personnel. In past emergencies, NESS managers have relied on the military to airlift supplies. However, the military's operational commitments can limit the availability of aircraft, so it cannot guarantee immediate transportation of NESS supplies. PHAC has not secured alternative airlift arrangements.

2.124 One exercise we reviewed noted the risks involved in shipping medical countermeasures by commercial aircraft. Officials told us that they are developing an agreement with the RCMP to ship emergency drugs in its aircraft.

2.125 We noted that as part of developing the National Emergency Response System, work is beginning on a National Emergency Transportation System (NETS). The NETS task is to address the need for a comprehensive transportation service within 24 hours. Public Safety and Emergency Preparedness Canada now has the lead in developing the NETS.

2.126 **Recommendation**. The Public Health Agency of Canada should co-ordinate the management of its National Emergency Stockpile System (NESS) with other federal agencies and include the NESS in the National Emergency Response System.

Public Health Agency of Canada's response. PHAC is working closely with Public Safety and Emergency Preparedness Canada on a number of fronts, including input into the development of the National Emergency Response System (NERS) and a National Health Emergency Management System. Part of that process will include ensuring that the NESS is closely linked to the emergency response activities outlined in the NERS.

2.127 **Recommendation.** Based on risk assessments and casualty scenarios, the Public Health Agency of Canada should update the contents of the national emergency stockpile as soon as possible. It should also secure arrangements for the transportation and distribution of supplies during emergencies.

Public Health Agency of Canada's response. PHAC is currently undertaking a strategic review of the NESS that includes a review of the contents of the stockpile. The strategic review, to be completed in 2006, will include risk assessments (initial risk assessment completed November 2004) and casualty scenarios. Emergency transportation of NESS supplies is being addressed through the National Emergency Transportation System (NETS).

PHAC' s Regional Emergency Response Co-ordinators will soon be developing NESS provincial and territorial emergency transportation plans in collaboration with each jurisdiction.

Use of the Special Access Program is inappropriate

2.128 Most CBRN medical countermeasures are not licensed for use in Canada; they are imported from the United States through the Special Access Program (SAP). For example, NESS managers use SAP to supply first responders with CBRN medical countermeasures. The Special Access Program was designed to give doctors access to drugs not licensed for sale in Canada, with control based on one doctor prescribing drugs for one patient. It was not designed for mass distribution of unlicensed drugs as medical countermeasures.

2.129 **Recommendation.** Health Canada should establish an appropriate legal structure for providing unlicensed drugs in an emergency.

Health Canada's response. Agreed. Health Canada proposes to develop the regulatory authorities, in consultation with stakeholders, to enable the Minister to authorize a block release of products that have not been approved for sale in Canada for the purpose of responding to public health emergencies. As well, Health Canada proposes to develop new regulatory authorities needed to authorize "emergency use" products for the medical countermeasures context.

Smallpox vaccine stockpile is still being completed

2.130 Following Budget 2001, Health Canada was allocated up to $48 million to develop smallpox vaccines and plans for their use and to purchase vaccine-related supplies. The use of smallpox virus as a biological weapon was identified as a risk, and scenarios were developed that projected up to

10 million casualties. In March 2003, a contract was awarded for the procurement of smallpox vaccine.

2.131 Due to problems in the manufacturing of the vaccine, Health Canada received only 5.7 million of the 10-million-dose requirement. It paid for only the doses it received. PHAC, now responsible for the stockpile, is not buying more vaccine to make up the shortfall; it is investigating the possibility of doing this by diluting the vaccine it has. At the time of our audit, it did not have in stock the 10 million doses identified as the required number.

2.132 Under the smallpox vaccine program, Health Canada was to negotiate with the provinces by April 2004 on plans to administer the vaccine. At the end of our audit in December 2004, the plans had not been completed by PHAC.

2.133 **Recommendation.** The Public Health Agency of Canada should determine how to meet its identified requirement for smallpox vaccine.

Public Health Agency of Canada's response. A decision on future procurement will be based on the results of the clinical trials of the current stockpile, a new risk assessment, and the results of the ongoing monitoring of smallpox vaccine research and development in 2006. In the interim, there is an adequate stockpile of smallpox vaccine and global commitment to assist in the event of an outbreak to ensure public safety and security.

A research and technology initiative needs to assess capacity gaps

2.134 The CBRN Research and Technology Initiative (CRTI) is a five-year, $170 million fund that Budget 2001 established to address CBRN threats. It involves 17 federal departments and agencies, led by Defence R&D Canada, an agency in National Defence. The CRTI is mandated to strengthen Canada's preparedness for, prevention of, and response to a CBRN attack. Funding (aside from $9.5 million for program administration) was divided among three main priorities: improving the technological capacity of federal laboratories ($27.5 million), accelerating the delivery of technology to first responders ($38 million), and investing in research and development ($95 million).

2.135 Forty federal laboratories participate in the initiative under a memorandum of understanding. We expected to find that the scheduling of investments in laboratory capacity had been guided by a risk assessment and gap analysis.

2.136 We found that between January and March 2002, a threat and risk analysis by the CRTI identified gaps in the federal laboratory capacity. Three clusters or groupings of departmental laboratories were then established according to their chemical, biological, or radiological/nuclear capabilities. The laboratory clusters identified the technologies or capacities that each was to develop. The CRTI Steering Committee then approved funding proposals based on an agreed-upon risk assessment.

2.137 Of the $27.5 million in total funding allocated to acquiring technology in federal laboratories, the CRTI committed 77 percent in the first two years

to addressing the identified gaps. But how all the labs will work together and use this technology in an emergency has not yet been clearly defined.

2.138 A Health Canada study of how the cluster of biological laboratories functioned during the September 2003 SARS crisis indicated that the clustering of laboratories improves the response to an emergency. The study report noted that more rapid analysis, and therefore more rapid prevention and mitigation measures, were possible because the cluster members involved in the incident were aware of the capacity and capabilities outside their organizations that they could call on to assist during the incident. We found that how the laboratories in the biological cluster and the chemical cluster will work together is still being developed. Cluster managers noted that the number of departmental response plans and the inconsistencies among them created problems for the laboratories in working together. They identified a tension between working together and supporting their operational mandates.

2.139 The CRTI was also mandated to accelerate the delivery of technology to the first responder community. It developed a risk analysis known as the consolidated risk assessment to prioritize projects, and we found the analysis to be adequate. The consolidated risk assessment is updated every year to guide the annual selection of projects.

2.140 By April 2004, the CRTI had funded 19 projects totalling $16.5 million to develop technology for first responders. It had also committed to funding 22 research and development projects totalling $17.1 million. These projects typically follow a two- to four-year cycle, with completion of the first projects scheduled for November 2004. However, Budget 2001 did not include funding to acquire equipment based on the technology developed or accelerated by the CRTI. The $10 million allocated in Budget 2001 for the purchase of CBRN equipment was for only two years, before any CRTI projects would be completed. The CRTI is not designed or mandated for mass distribution of technology to first responders.

Federal programs for first responders have progressed slowly

2.141 Budget 2001 allocated funds to build a response capacity not only in federal departments but also at the local level. It set aside $59 million over five years for CBRN training of first responders, $20 million over five years to develop a national capability for heavy urban search and rescue, and $10 million over two years to buy CBRN detection and decontamination equipment and protective clothing for first responders.

2.142 **Consulting first responders.** In late 2001, officials from OCIPEP, the Department of the Solicitor General, and National Defence met with first responders in eight Canadian cities. Their aim was to develop ways of strengthening the national capability to manage the consequences of terrorist attacks. The report that summarized these meetings noted the urgent need for a clear federal policy on enhancing the capacity of first responders to deal with a CBRN incident. It concluded that no jurisdiction had the capacity to deal with mass casualties.

2.143 The report stated that training was the most critical part of preparing for CBRN threats, and it was lacking across the country. All first responders, including health care professionals, needed basic training in CBRN awareness. Further, federal leadership was urgently needed to establish training standards or guidelines so that all those who received training would be trained to the same degree. Standardized training was seen as the way to ensure that different jurisdictions could co-ordinate an integrated response.

2.144 First responders were said to be looking to the federal government to establish standards or guidelines for equipment as well. The report said it was clear that first responders were aware of the need to ensure that their equipment could interoperate with that of other jurisdictions when necessary.

2.145 The report also said that the current arrangement for funding first responders' CBRN equipment (including heavy urban search and rescue equipment) through the Joint Emergency Preparedness Program was too slow and cumbersome to be effective. It contended that a major overhaul of the program as it existed then was necessary for the timely provision of equipment. Furthermore, any funding model should take into account maintenance and longer-term replacement costs and allow for flexibility.

2.146 We spoke with first responders primarily at the municipal level. We learned that they are well aware of the need to work together. First responders told us about new initiatives and co-operation agreements and protocols. They have developed new plans and revised others. In addition, PSEPC officials explained that they have held cross-country consultations aimed at improving program delivery and have been working to improve the delivery of funds.

2.147 **Heavy urban search and rescue (HUSAR).** Heavy urban search and rescue capacity is the location and removal of trapped persons in collapsed structures, using dogs and sophisticated search equipment. HUSAR capacity has increased slowly.

2.148 Budget 2001 allocated $20 million over five years to develop a capacity for search and rescue in eight major cities. This investment was managed through an existing shared-cost program; the federal share was 75 percent. Under the Joint Emergency Preparedness Program (JEPP), the federal government co-funds provincial proposals. Shared funding of HUSAR equipment has proved to be problematic because of its high capital cost and the continuing costs to the municipalities of operating and maintaining it. Even a 75-percent federal share of the capital expenditure has proved insufficient to allow municipalities to take up the federal funds available. We found that at 1 April 2004, the provinces, territories, and municipalities had used less than 50 percent of the available funds.

2.149 We expected to find funding targeted to high-risk communities and guidance provided to them on identifying the capacity they need.

2.150 We found that the former OCIPEP had developed HUSAR team profiles and identified the needed equipment. Proposals by the cities for HUSAR funding were approved based on an analysis of the gap between

existing and targeted capacities. Highest priority was assigned to five of the eight cities identified in the initial risk assessments. A sixth team is being developed, and the remaining two cities have expressed an interest in participating.

2.151 **Providing CBRN equipment to first responders.** OCIPEP used its existing Joint Emergency Preparedness Program (JEPP) to fund the purchase of $10 million in CBRN equipment for provincial and municipal first responders. It chose JEPP as the funding vehicle because, as an existing program, it could deliver funding quickly. The funding was for only two years, and the funds for the first year were received in the last quarter of the year.

2.152 OCIPEP received proposals from all provinces and one territory; their costs would total more than the $10 million available. Since the federal response is to support provincial and local authorities, we expected to find a list of provincial and municipal resources and capabilities—information that would then guide the distribution of federal funding to develop local capacities in areas most at risk. The information could also be used to develop goals for national preparedness, along with measurable performance indicators.

2.153 We did not find a risk analysis to guide funding decisions. We found that OCIPEP had not developed performance benchmarks for CBRN response teams or identified gaps in the response capacities of high-risk communities. Officials informed us that OCIPEP had relied on the expertise of provinces and territories to identify gaps in their respective jurisdictions. Rather than develop, fund, and equip a national first response capacity in a select number of cities as it did for HUSAR, OCIPEP spread the funding across regions, thereby diluting the response capacity.

2.154 Halfway through the two-year program, the CBRN Steering Committee began using provincial population percentages to guide its allocation of funds. OCIPEP officials told us that this was meant to achieve proportionate distribution of the funds across the country. However, we found that in the first year, the funds had been allocated to the provinces that had submitted proposals first. Early allocations to provinces with low populations meant that funding by provincial population percentages was not achieved. Moreover, this approach was not based on risk.

2.155 Although provincial populations were used to allocate funding, the funds were not then directed to the high-population centres in the provinces or to areas of highest risk. Across the country, cities with populations below 300,000 received 40 percent of all the funds.

2.156 **Equipment guidance is lacking.** We expected that to help first responders make informed choices in their purchase of off-the-shelf response equipment, the federal government would provide guidance on equipment as a means of creating a national **"surge" capacity**. Ideally, the types of equipment used by response teams across the country—protective equipment; chemical, biological, and radiological detectors; and communications equipment—would be compatible and interoperable with

Surge capacity—Surge capacity refers to the ability of emergency response services to aid and support each other. Mutual aid can encompass the personnel, equipment, and resources need to provide relief to overwhelmed emergency services during a major incident. Interoperability and compatibility of protective equipment may be critical in large incidents, as in the case of respirators at the World Trade Centre in September 2001. Promoting the standardization of protective equipment would support equipment sharing in the field among response services. It would make the use of supplementary equipment delivered to a major event site (from federal caches, for example) possible as well, by assuring its compatibility with existing gear and requiring less training and fitting in the field.

Source: Protecting Emergency Responders, Santa Monica, CA RAND Corporation, 2003

equipment in other jurisdictions. But because standards were not available, we expected to find a list of recommended equipment as a resource for responders at all levels of government. It should be noted that in 2002, performance standards for civilian use of CBRN equipment were not readily available. PSEPC officials also pointed out that the international community is struggling to develop technical standards for CBRN equipment and that the community considers this to be a long-term problem.

2.157 Based on its consultations with local first responders, the federal government knew they needed its leadership in developing a response to terrorism. When OCIPEP first announced that CBRN equipment would be funded, it said it would develop national guidelines for the acquisition of equipment and training—guidelines that were never developed. While OCIPEP had gathered some information on best practices for CBRN teams, it did not share the information with the provinces during the JEPP funding process. It offered only ad hoc advice on equipment selection. In summer 2004, officials said they were concerned that recommending specific types of response equipment could create a liability for the federal government.

2.158 Each province submitted its own proposals for equipment purchases, specifying the type and quantity of equipment its response teams needed. In the absence of federal guidelines on performance and cost, we found a wide variation in the types and cost of equipment purchased across the country.

2.159 For example, the costs of Level A suits to protect against chemical and biological hazards ranged from $700 to $7,200, with no explanation of the cost difference. Different jurisdictions bought different detectors that provided different levels of performance at different costs. One city purchased a complex chemical detector for $180,000. However, its proper operation requires highly specialized training and ongoing maintenance and, in a recent incident, the municipality could not operate the detector properly and had to request the RCMP's assistance. The municipality has since shelved the detector because it could not dedicate the resources needed to operate it properly.

2.160 We found a considerable variation in the capabilities of the CBRN equipment purchased and in the training required for its proper operation. These variations would translate into problems with interoperability and surge capacity. We noted differences, for example, in the protection levels and wearing times of various suits and breathing apparatus and in the ability to reliably detect and quantify a broad spectrum of chemical and biological agents.

2.161 **A new strategy has been developed.** PSEPC recently developed a draft national strategy for responding to CBRN incidents. Its objectives include working with provincial and territorial governments, standards organizations, and industry to develop equipment capability standards and guidelines for CBRN agents. To meet this objective, the CRTI and PSEPC will provide support for the building of a testing and evaluation capability at the Counter-Terrorism Technology Centre (CTTC) in Suffield, Alberta, for use by the first responder community, governments, and industry.

2.162 In October 2004, the CBRN Research and Technology Initiative began discussions with the CTTC the on how to conduct testing and evaluation of CBRN equipment and technologies. Any standards would be communicated by PSEPC to the first responder community.

2.163 **Recommendation.** Public Safety and Emergency Preparedness Canada should lead the development of nationally accepted standards for equipment used in responding to chemical, biological, radiological, and nuclear threats. It should also work toward creating unified standards with the United States.

Public Safety and Emergency Preparedness Canada's response. Work is already underway, PSEPC is collaborating with the Chemical, Biological, Radiological and Nuclear Research and Technology Initiative (CRTI) to develop national chemical, biological, radiological, and nuclear (CBRN) equipment standards in Canada. PSEPC and the CRTI are currently developing a framework to guide work in this area, in co-operation with all key stakeholders, including other federal government departments, provinces and territories, the U.S. Department of Homeland Security, industry, standards development organizations, and first responders.

2.164 **Little training completed for first responders.** Budget 2001 allocated $59 million over five years to the training of first responders; six departments, led by OCIPEP, were tasked with developing a CBRN training program for first responders. Of the Budget funding, $11.2 million was allocated to OCIPEP's Emergency Preparedness College and $21 million to Health Canada. We expected to find training programs based on risk assessments, with their delivery structured to ensure that training was timely and efficient.

2.165 We found problems with the CBRN first-responder training program. Federal training has been delayed significantly, and only a small number of first responders have been trained in Canada's major urban centres. The structure of the training is also a concern.

2.166 The Emergency Preparedness College, in partnership with the other federal departments and agencies, was to design and deliver the joint CBRN training program. A four-level program of CBRN courses was designed, with the first two levels (awareness and basic training) focussed on raising awareness of a CBRN incident and surviving exposure to CBRN agents. The next two levels (intermediate and advanced) deal with intervening in and neutralizing the event and are directed to the traditional first responders in fire, police, and emergency medical services. Health care providers such as hospital workers were not included in the College's specialized CBRN-response courses, even though the submission requesting funding for the training program had specifically identified the specialized training needs of health care workers.

2.167 We expected that a training plan and schedule would be linked to threat scenarios and associated casualties, that training of higher-risk cities would be addressed as a priority, and that a timeline would be established for achieving the desired capacity. Although the College did not request a formal threat and risk assessment by region until April 2004, it did use available

intelligence to identify higher-risk cities and did give them priority in initial access to training. The problem that arose was in the volume of delivery of the training.

2.168 The lowest levels of training are the introductory and basic courses, which familiarize first responders with threats but do not teach mitigation techniques. The joint training group estimated that about 100,000 first responders required the basic level of training. By October 2003, the College had piloted its basic course in Fredericton, New Brunswick, and in Winnipeg, Manitoba. The College told us it has also trained 176 trainers to give the basic course. To date it has issued 474 training kits to these instructors. Subsequently, the College planned to deliver the kits on CD-Rom. It has now informed us that the course will be delivered through e-learning on the Web. The College also proposes to deliver its introductory course on the Web.

2.169 The higher-level courses are aimed at training first responders in how to work in a CBRN environment. A strategy has not been developed to link the training needs of a first responder team to a target level of response capacity. Nor has the College addressed the need for refresher training and retraining to allow for staff turnover.

2.170 The course design suffered from the fact that a concept of operations for dealing with a CBRN event was not developed. Neither the Emergency Preparedness College nor its CBRN courses currently provide training in the incident command system, even though a number of provinces use such a system to govern their response to a CBRN event as well as PSEPC's new National Emergency Response System (NERS).

2.171 The funding request stated that OCIPEP would co-ordinate the CBRN training initiative in collaboration with the RCMP, Health Canada, National Defence, and others. We were told that Health Canada started developing its own course for medical personnel in July 2003.

2.172 The request for training funds estimated the target population for the intermediate course at 6,000 first responders, with 2,000 targeted for the advanced course. The College, with its federal partners, does not have an adequate plan to deliver timely intermediate and advanced CBRN training to the first responders it identified who need training. By fall 2004, the College had given 134 first responders its intermediate course and 63 its advanced course. The College plans to provide the intermediate course in Ottawa five times a year and hopes to expand its offerings in the future.

2.173 **Recommendation.** Public Safety and Emergency Preparedness Canada, together with the other federal departments and agencies mandated to train for chemical, biological, radiological, or nuclear response, should revisit the objectives for providing training to first responders and the delivery of the training.

Public Safety and Emergency Preparedness Canada's response. A CBRN Strategic Review group has been formed and tasked with addressing key issues related to the development and delivery of CBRN training. The anticipated result is a strategic plan that will address the objectives, delivery,

tracking, and accountability measures for this program. The completion date for the plan is scheduled for the end of 2005.

Federal strategy needed for exercising response plans

2.174 We expected that federal response plans would be tested and exercised regularly and revised according to the results.

2.175 The National Security Policy has called for the staging of regular national and international exercises involving civilian and military resources, in order to assess the adequacy of the national system in various emergency scenarios. In our opinion, the regular testing and exercising of response plans is critical to their effectiveness.

2.176 Departments have tested components of their response plans; we found several national exercises conducted since September 11, 2001. While federal departments have participated in exercises that integrated the federal response to a CBRN attack with the provincial and municipal responses, we found no federal strategy or criteria to guide the federal government's participation. We found delays and gaps in the post-event analysis and implementing of recommendations. For example, the final analysis of the TOP OFF II exercise, a U.S.-Canada simulation exercise for senior officials, was circulated 13 months after the exercise.

2.177 Budget 2001 did not allocate resources to exercises or to training of emergency managers. We could not find funds set aside subsequently at the program level to budget for conducting exercises. We were told that any funds used so far in conducting exercises were taken from other programming. For example, the former Department of the Solicitor General used some of its training money to pay for TOP OFF II exercises.

2.178 As part of the new PSEPC structure, a National Exercise Division has been created. It will be responsible for developing guidelines on conducting exercises.

2.179 **Recommendation.** Public Safety and Emergency Preparedness Canada should develop a long-term plan and budget for the conduct of national exercises.

Public Safety and Emergency Preparedness Canada's response. An Exercise Division has been created within PSEPC, and work is already underway to develop a long-term plan and funding strategy for a National Exercise Program. This will be a multi-step process that will require consultation and validation while continuing to deliver complex international initiatives such as Exercise Triple Play. A key part of the National Exercise Program will be the ongoing consolidation of lessons learned and how they inform the establishment of future priorities.

Spending on critical infrastructure protection was not managed well

2.180 Critical infrastructure is the backbone of Canada's economy; it is essential to the health, security, safety, and economic well-being of Canadians and the functioning of government. Critical infrastructure includes energy

and utility systems, communications and information technology, financial systems, health care, food, water, transportation, safety services, government, and manufacturing capacity.

2.181 Budget 2001 allocated $190 million to a new program for emergency preparedness and critical infrastructure protection (EP/CIP) co-ordinated by OCIPEP across 12 departments. Half of those funds were allocated to OCIPEP.

2.182 The purpose of the EP/CIP program was to expand the capacity of federal agencies to protect the country's critical infrastructure from attack. We expected to see that the program funds had been allocated on the basis of a risk analysis.

2.183 No threat and risk assessment was carried out before the funds were allocated. A committee of officials was formed that considered proposals from departments and agencies and made a recommendation to the Treasury Board.

2.184 We looked at the three agencies that received the largest share of the money: OCIPEP, the Communications Security Establishment, and the RCMP combined accounted for 80 percent ($152.5 million) of the total budget. We found that

- the targeting of the Communications Security Establishment's allocation was based on reasonable criteria; and
- the RCMP is using its funding to expand existing cybersecurity programs, which is consistent with its approval from the Treasury Board.

2.185 We found that funds allocated to OCIPEP were directed to five thematic initiatives:

- putting the Government of Canada infrastructure house in order;
- enhancing federal, provincial, and international partnerships;
- enhancing national operational capacity;
- developing and implementing targeted programs; and
- strengthening the policy framework.

What we could not find was evidence of a risk analysis to show how the decision was made to give OCIPEP half of the $190 million or how that amount was allocated to the five initiatives.

2.186 As part of the overall program, OCIPEP was to perform a co-ordinating function. It was to work with the Treasury Board Secretariat to recommend the allocation of funds to individual departments. It was also responsible for reporting annually to the Treasury Board Secretariat on how the EP/CIP program was performing.

2.187 At the time of our audit, OCIPEP had compiled one integrated annual report on the critical infrastructure protection program of the public safety and anti-terrorism initiative, as required. We found that since it was the initial report, much of the activity reported involved attendance at meetings

or the development of planning frameworks. OCIPEP held three meetings in 2003 to discuss a common evaluation framework. That framework has been developed. We did not find evidence that any additional co-ordinating meetings were held.

2.188 Information for the second report was due from departments in September 2004. However, the Treasury Board Secretariat issued a revised reporting template on 17 December 2004.

2.189 Officials were unable to say how much money OCIPEP had spent on the critical infrastructure protection program and how much funding had lapsed. We interviewed staff from OCIPEP, National Defence, and PSEPC, and no one was sure whether funding had been deferred to subsequent years or had been absorbed into other programs. Program staff told us that in the first two years they thought they had lapsed $10 million of a $35 million budget, but we were unable to verify this.

2.190 We were able to determine that part of the problem in tracking expenditures was the failure of OCIPEP staff to charge their work to the correct financial codes. Management could not correct this problem. In our opinion, basic management controls were missing. We were told that the program may not recover the lapsed funding.

2.191 PSEPC has acknowledged that problems did occur in the past. It has undertaken to develop a co-ordinated strategic plan that establishes goals and priorities for enhancing capacity; to monitor the plan's implementation; to identify and address gaps in emergency preparedness; and, based on established standards and guidelines, to evaluate the effectiveness of expenditures.

2.192 We support PSEPC's proposed solution to the problems we have identified.

2.193 **Recommendation.** Public Safety and Emergency Preparedness Canada should revisit its programs for the emergency preparedness and management of the nation's critical infrastructure protection and base its strategy on a risk assessment.

Public Safety and Emergency Preparedness Canada's response. PSEPC is currently working with its partners (other government departments, provinces, territories, private sector, and U.S.) to develop a national strategy and work plan based on risk management. A consolidated critical infrastructure protection (CIP) risk assessment is challenging because of the different states of preparedness and security of each of the 10 national critical infrastructure sectors. Federal officials (including PSEPC staff) have worked with their U.S. counterparts to develop CIP risk assessment methodologies for the implementation phase of the Canada-U.S. Public Security Technical Program (PSTP). The results of these methodologies will guide work on risk assessments in both countries and be one of the contributions to our respective and complementary national CIP strategies.

Conclusion

2.194 The creation of Public Safety and Emergency Preparedness Canada has begun the process of integrating and advancing emergency preparedness programs. However, due to the relative newness of the current organization, much remains to be done.

2.195 Prior to the reorganization, funding for first responders under the Budget 2001 anti-terrorism initiative suffered from the poor sequencing of programs. The enhancement of response capacity is a function of procedures, equipment, and training, all working together. The federal training programs lagged behind the provinces' equipment purchases, and the strategy to co-ordinate and integrate the responses of different levels of government and regions is still being developed. Under the initiative's funding, each component was developed separately when, instead, they should have been developed to reinforce each other.

2.196 Funds for first responder equipment purchases were disbursed without reference to a threat and risk analysis, and the result was a poor allocation of those funds. We found that equipment purchased for similar needs varies widely in cost and quality. Most critically, the opportunity was not taken to create a national pool of compatible, interoperable equipment.

2.197 Although first responders cited training as their primary need, after significant expenditures the federal program has trained few first responders at the intermediate and advanced levels. Again, threat and risk analyses were not used to establish program goals.

2.198 The new Public Safety and Emergency Preparedness Canada faces many challenges to achieving the goals set for it by government. It will be important to ensure that the Department has the appropriate authorities, structures, and resources necessary to address current and future problems. Senior management is aware of both the challenges and the need to avoid the circumstances that contributed to the problems encountered by OCIPEP over the course of that organization's existence.

2.199 Moreover, the new department needs to review many of the decisions taken by OCIPEP. In our opinion, without strong and clear support from all areas of the federal government, PSEPC will be years away from meeting the goals it has established and that have been established for it. And the gaps in Canada's ability to respond to an emergency will remain.

2.200 We also assessed the extensive improvements made to air transport security. Transport Canada did not meet our audit criteria in its oversight of the air transport security system. It has expanded the security inspection service and improved training; however, we could not conclude whether the number of inspectors and the frequency of inspections are appropriate, as the program has not been based on a documented risk analysis. The security inspection and enforcement regime was not designed to regulate federal agencies such as CATSA, the Canadian Air Transport Security Authority.

2.201 CATSA was created to manage and deliver many components of air travel security that were dramatically expanded by the 2001 Budget initiative. About $1 billion has been spent to acquire and install equipment to screen for and detect explosives. We found that the implementation of the Explosives Detection Systems program has proceeded well to date.

2.202 We found that the marine security programs have made good progress and met most of our criteria. We noted that threat and risk analysis was used as a basis for allocating funds to priority areas. However, additional expenditures will likely be required to fill gaps in capabilities. The implementation of the International Ship and Port Facility Security Code is generally proceeding well, though here, too, success may depend on the availability of resources in the future.

About the Audit

Objectives

The objectives of the audit were to determine whether

- Transport Canada's oversight of the air transport security system is adequate;
- Transport Canada and the Canadian Air Transport Security Authority (CATSA) have adequately managed those elements of Explosives Detection Systems acquisition and implementation for which they are responsible;
- marine surveillance capital projects have been adequately managed and the International Ship and Port Facility Security Code implemented according to the government's plan; and
- emergency preparedness programs of the federal government are adequately managed.

Scope and approach

This audit was the second of two audits of the government's National Security Enhancement Initiative presented in Budget 2001. The report on the first audit was tabled in March 2004. This report on the second phase addresses the integrity of the air transport security system as a whole; capital expenditures on Explosives Detection Systems and marine security surveillance systems; the implementation of the International Ship and Port Facility Security Code; and emergency preparedness programs.

The audit focussed on the departments and agencies involved in implementing or monitoring these programs. They included

- Canadian Air Transport Security Authority
- Fisheries and Oceans Canada (specifically, the Canadian Coast Guard)
- Health Canada
- National Defence
- Office of Critical Infrastructure Protection and Emergency Preparedness
- Public Health Agency of Canada
- Public Safety and Emergency Preparedness Canada
- RCMP
- Solicitor General Canada
- Treasury Board Secretariat
- Transport Canada

Our audit was limited to federal programs and did not include emergency preparedness plans and capabilities of other levels of government.

Criteria

Our audit was based on the following criteria:

- The air transport security system should be based on an adequate risk assessment.
- Transport Canada should take adequate measures to ensure compliance with its security regulations, including
  - adequate training and numbers of inspectors;
  - adequate frequency of inspections;
  - quality control of inspections;
  - analysis of breaches;
  - corrective action of recurring and systemic problems.

- Equipment and contracting options should have been appropriately assessed.
- There should be time and cost controls and reporting commensurate with an undertaking whose capital costs exceed $100 million.
- Equipment acquired should meet Transport Canada's standards and objectives as stated in acquisition plans and contract specifications.
- Operators should meet Transport Canada's standards for the detection of simulated threats and threat image projection.
- Transport Canada should mitigate the risks that implementing EDS poses for the smooth functioning of the air transport system as a whole.
- Projects should comply with best practices and standards of project management.
- Departments should ensure that best practices for contracting are observed and that contracting regulations are followed.
- There should be a clear chain of command for the federal and national response to incidents.
- Federal response plans should be based on threat/risk assessments.
- Federal response capabilities should be matched to approved threat and casualty scenarios.
- There should be federal equipment guidelines for first responders, specifying minimum performance and interoperability requirements as well as test protocols.
- First responder training should
  - be linked to current threat/risk assessments;
  - be timely;
  - be targeted and prioritized;
  - include cyclical retraining.
- Federal response plans should
  - be tested and evaluated regularly;
  - be integrated across levels of government;
  - be revised according to post-event and post-exercise analysis.

Audit team

Assistant Auditor General: Hugh McRoberts
Senior Principal: Peter Kasurak
Principal: Gordon Stock
Director: Edward Wood

Dawn-Alee Fowler
Anthony Levita
Carol McCalla
Mark Carroll
Sami Hannoush
Steven Mariani
Jacinthe Pépin

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—April 2005

Main Table of Contents