Chapter 25

Preparedness for Year 2000

Final Preparation

Table of Contents

Exhibits

Preparedness for Year 2000

Final Preparation

Main Points

25.1 The government has made significant progress in preparing its systems that support government-wide mission-critical functions for the Year 2000 computer problem. The Treasury Board Secretariat reported that work on government-wide mission-critical systems was 99 percent complete at July 1999. Our audit supports the overall 99 percent completion rate for those systems. According to its plans, all government-wide mission-critical systems were to be ready for Year 2000 by 31 October 1999, two months before the new millennium.

25.2 Health Canada and the Atomic Energy Control Board have established Year 2000 requirements for licensees of medical devices, nuclear power reactors and radioactive devices. Some follow-up is needed for medical and radioactive devices but the licensees for active nuclear power plants have met the requirements.

25.3 Measures are being put in place for contingencies and national emergencies. Although contingency procedures have largely been defined, departmental contingency planning needs more work.

25.4 We concluded that the government needs to remain vigilant to keep any Year 2000 disruptions to a minimum.

Background and other observations

25.5 Year 2000, the two-digit year code problem, has been a cause of concern to industry and governments around the world. The estimated costs of addressing this problem run as high as US$800 billion worldwide. In August 1999, the federal government estimated the costs of its Year 2000 projects at $2.2 billion. According to the Treasury Board Secretariat, the final costs could reach $2.5 billion.

25.6 In 1997 we audited the government's preparedness for Year 2000, and again in 1998. Our 1997 Report noted our concern about the slow pace of Year 2000 work; in 1998, we remained very concerned that some essential services might be interrupted in 2000. Most of our recommendations have been accepted and implemented by the government.

25.7 In 1999, as we completed our work in individual departments and agencies, we reported our findings to management and suggested actions to consider. That additional step was taken to provide more time for departments and agencies to act.

25.8 We verified the government's Year 2000 progress information as reported by the Secretariat against the information in its supporting files and we further reviewed departmental documents for seven government-wide mission-critical functions in six organizations. Our verification showed no substantive differences from the information reported by the Secretariat.

25.9 In the departmental contingency plans we reviewed, we found that some key components were not complete or lacked specific details. In particular, plans for testing were weak and few organizations planned to complement the National Contingency Planning Group validation exercise with other tests of their contingency procedures.

25.10 We have identified several issues that will require action beyond 1999, and have recommended measures for the government to take or to consider. They include moving to comply with government date standards; maintaining and updating valuable information bases developed from Year 2000 projects; and looking out for Year 2000 pitfalls after January 2000.

The government's responses to our recommendations are included in the chapter. The government agrees with our recommendations and the responses identify the action that it will take to address them.

Introduction

25.11 The Year 2000 computer problem, often called the millennium bug or Y2K, refers to the potential for systems error, malfunction or failure caused by the past practice of representing the year with a two-digit code. Given the ever-increasing reliance on information technology, the Year 2000 threat extends to virtually all organizations in both the private and the public sectors around the world.

25.12 Because of the significance of its potential impact, we conducted two previous audits of the federal government's preparedness for Year 2000. In 1997, we audited the government's overall state of preparedness; in 1998, we focussed on the preparedness of systems that support government-wide mission-critical (GWMC) functions. The GWMC systems are those that the government considers essential to the health, safety, security and economic well-being of Canadians.

25.13 In our October 1997 Report, we were concerned about the pace of remediation work and the serious threat of Year 2000 to essential programs and services. In December 1998 we reported that while the pace of Year 2000 work had accelerated, the threat to some GWMC functions remained.

25.14 In that second Report, we recommended that Year 2000 continue to be a top priority for the government and that the related work be further accelerated. We emphasized the need for contingency planning and for the testing of those plans. We also encouraged the government to improve its government-wide monitoring of Year 2000 progress and its reporting of that progress to Parliament.

25.15 In 1997, when we started our Year 2000 audits, there had been few media reports on the subject. Many organizations, including some government departments and agencies, had not proceeded much beyond the planning and inventory phase of their Year 2000 projects. At that time, one information technology research firm had estimated that the costs of addressing Year 2000 could reach US$600 billion worldwide.

25.16 Thus far in 1999, the millennium bug has received widespread attention by the media and the level of public awareness in Canada and the United States has been high. Banks and utility companies have been reporting readiness and providing assurance to their customers. Estimates of Year 2000 costs worldwide now reach over US$800 billion. The federal government's 1997 estimate of $1 billion for Year 2000 costs was revised to $2.2 billion in August 1999. The Treasury Board Secretariat has advised us that overall costs of Year 2000, including contingency planning and measures, could approach $2.5 billion.

The overall costs of Year 2000 for the government, including contingency planning and measures, could approach $2.5 billion.

25.17 In 1999, the priority for most organizations has been to complete their final preparation for Year 2000.

Focus of the audit

25.18 Our current audit focussed on the government's final preparation for Year 2000. In particular, we audited three areas — readiness through government-wide monitoring and reporting of progress in GWMC systems and contingency planning; regulatory responsibilities; and national emergency preparedness.

25.19 To examine the government's readiness, we interviewed staff and reviewed files at the Treasury Board Secretariat and at six organizations that are responsible for seven government-wide mission-critical functions. We did not audit the readiness of departmental mission-critical systems. We selected two areas of regulatory responsibilities — medical devices at Health Canada and nuclear facilities and radioactive devices at the Atomic Energy Control Board. With respect to national emergency preparedness, we audited the National Contingency Planning Group and Operation Abacus at National Defence.

25.20 Our audit work was not designed to provide assurance that the government will be able to deliver all mission-critical functions in 2000. The government remains responsible for its systems and their ability to continue to function properly beyond 1999. The purpose of this chapter is to provide information on the action that the government has taken to address Year 2000 and the observations we made during the audit. Further information about the audit objectives, scope and criteria can be found at the end of the chapter in **About the Audit**.

Observations and Recommendations

Government Readiness

Significant progress has been made in preparing government-wide mission-critical systems

At July 1999, the overall completion index for systems supporting government-wide mission-critical functions was 99 percent.

25.21 In 1996, the Treasury Board Secretariat established a Year 2000 Project Office under its Chief Information Officer Branch to provide leadership in addressing Year 2000 issues in government. As we concluded our 1997 audit, the Secretariat advised us that it planned to monitor the Year 2000 progress of critical systems across the government. In the fall of 1997, it established a list of functions that were considered mission-critical across the government and began to request regular information on progress from the departments and agencies responsible for those functions.

25.22 The Secretariat adapted the methodology of a large information technology research and consulting firm. It set target dates for Year 2000 remediation, testing and implementation of systems that support the government-wide mission-critical (GWMC) functions. The target date for their full completion was 30 June 1999.

25.23 Since January 1999, the Secretariat has been monitoring and reporting monthly on the Year 2000 progress of systems that support 43 government-wide mission-critical functions. On 26 August 1999, its last monthly report on Year 2000 progress at July 1999 noted that the overall completion index for systems supporting GWMC functions was 99 percent.

25.24 In the current audit, we noted that Year 2000 has become a priority issue for senior management. Since June 1998, when the completion rate was 50 percent, the government has made significant progress in making the critical systems compliant for Year 2000. Exhibit 25.1 shows the progression of the overall completion index since September 1997, when the Secretariat first started surveying departments and agencies and compiling data on Year 2000 progress.

25.25 The 26 August report of the Secretariat showed that 25 of the government's 43 GWMC functions had reached 100 percent completion. Another 13 were at 99 percent and 3 were at 98 percent. Systems for two of the functions were about 95 percent complete. The functions and their completion rates are shown in Exhibit 25.2.

Our review showed no substantive differences

25.26 In response to our 1998 recommendation to seek independent validation of information on progress, the Secretary of the Treasury Board wrote to deputy ministers and heads of agencies, suggesting that they assign their internal audit staff to undertake the validation. In May 1999, the Secretariat provided the government's internal audit community with further guidance on independent validation.

25.27 We reviewed the August 1999 progress report prepared by the Secretariat and verified the information against supporting data and files at the Secretariat. We further verified the Secretariat's information against the records and files of six organizations that are responsible for seven GWMC functions. We also reviewed their contingency plans for the functions we had selected for audit. With the exception of the export and import controls function, the functions were selected on the basis of their criticality. The export and import controls function was selected because it ranked last in the completion index — 94 percent at July 1999. The six organizations and the seven GWMC functions we audited are:

- Canadian Broadcasting Corporation — emergency broadcasting;
- Environment Canada — weather forecasting;
- Foreign Affairs and International Trade — export and import controls;
- Human Resources Development Canada — income security; employment insurance;
- Public Works and Government Services Canada — Receiver General; and
- Revenue Canada — income tax processing.

As we finalized this report, Foreign Affairs and International Trade advised us that systems supporting the export and import controls function had been fully implemented in early September 1999.

25.28 The Secretariat provided us with a draft version of its August 1999 progress report. We conducted a cursory review and communicated our comments and concerns to Secretariat staff. The Secretariat addressed the issues and revised the report before its release on 26 August. Our subsequent review of the report revealed no major discrepancies between its content and the Secretariat's supporting files.

Our review of the Secretariat's progress report revealed no major discrepancies between its content and the Secretariat's supporting files.

25.29 Further, we noted that where system testing and full implementation of repaired systems had yet to be completed at July 1999, all key activities were planned for completion by October 1999. The Secretariat has assured us that it will continue to monitor GWMC functions and that it will focus on organizations that have yet to fully complete the testing and implementation of compliant systems. The Secretariat also stated in its August 1999 progress report that it will keep Canadians informed on its Year 2000 activities as the situation evolves. We have asked the Secretariat to keep us up-to-date on Year 2000 progress.

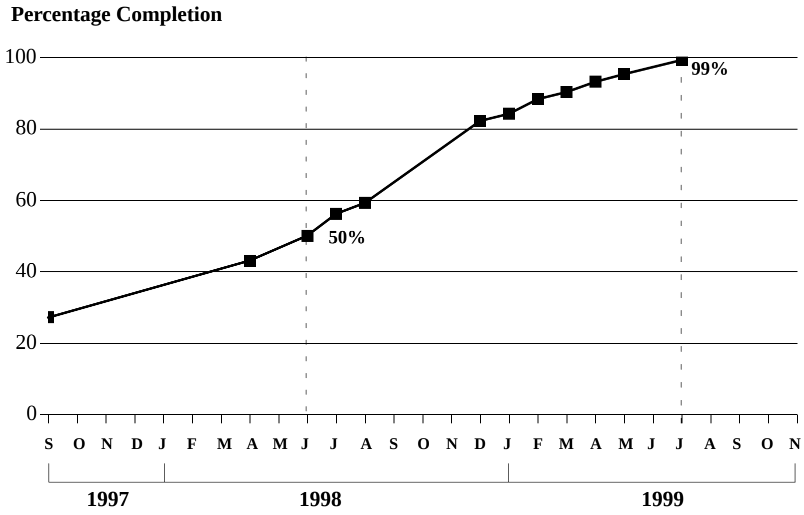


Exhibit 25.1

Year 2000 Progress of Systems Supporting Government-Wide Mission-Critical Functions

Source: Treasury Board Secretariat

Exhibit 25.2

Government-Wide Mission-Critical Functions and Their Year 2000 Completion Status

Department, Agency or Crown Corporation	Function	Completion Index (percentage)
Atomic Energy of Canada Limited	• control, safety, monitoring and facilities management	100
Canadian Broadcasting Corporation	• communications and broadcasting system	99
Canadian Food Inspection Agency	• food production and inspection	99
Canadian Heritage (Parks Canada)	• maintenance management system	98
Canadian Security Intelligence Service	• security intelligence • security screening	99 99
Citizenship and Immigration Canada	• managing access to Canada	99
Communications Security Establishment	• foreign intelligence and information technology security	100
Correctional Service Canada	• offender reintegration	100
Environment Canada	• environmental forecasting system	99
Fisheries and Oceans	• environmental response activities • flood control • marine traffic safety • search and rescue	100 100 99 99
Foreign Affairs and International Trade	• consular affairs • export and import controls • Canadian passport office • network (messaging system)	100 94 100 95
Health Canada	• laboratory centre for disease control • therapeutic products program • food program • environmental health program • medical services	100 100 100 100 100
Human Resources Development Canada	• income security • employment insurance	100 100
Indian and Northern Affairs Canada	• band support funding	100
Department of Justice	• family orders and agreements enforcement	98
National Defence	• defence of Canada/deployed international operations • domestic operations	99 99
Natural Resources Canada	• aeronautical and technical services • seismic monitoring • geomagnetic monitoring	100 100 100

(continued)

Exhibit 25.2

(continued)

Department, Agency or Crown Corporation	Function	Completion Index (percentage)
Public Works and Government Services Canada	• public service compensation • Receiver General services • processing government financial transactions	100 100 100
Royal Canadian Mounted Police	• law enforcement	99
Revenue Canada	• social income redistribution • income tax processing • customs border services and trade administration	100 100 100
Tax Court of Canada	• appeals management system	100
Transport Canada	• transport regulation	99
Veterans Affairs Canada	• health care • pensions and allowances	98 99

Source: Treasury Board Secretariat, August 1999

25.30 In our review of Year 2000 remediation work and test results at the six organizations, we found no substantive differences from the information reported by the Treasury Board Secretariat. We noted some areas where improvements were possible and communicated them to the organizations in September 1999 for their consideration and action. They included such issues as further testing of external interfaces; independent testing of repaired program code; documentation and accessibility of test results; and documentation of full system accreditation and certification for Year 2000. Subsequently, management of the organizations advised us that it had considered our observations and findings, and some had started to address them.

Contingency planning was not fully complete and more testing of the plans was needed

25.31 There can be no guarantee that repaired and compliant systems will function fully after 1999. Undetected errors could exist; other infrastructures on which systems depend but that are outside the direct control of departments and agencies could fail. Thus, contingency planning is an essential and prudent measure for addressing Year 2000.

25.32 In 1998, we recommended that contingency plans be developed and tested prior to 2000. The Secretariat established requirements in 1998 for risk assessments and high-level contingency plans. In 1999, the Secretariat and the National Contingency Planning Group jointly set target dates for all 23 departments, agencies and Crown corporations that are responsible for GWMC functions to complete various components of contingency plans. All key components of those plans were to be completed by April 1999 and submitted for review to the Secretariat and to the National Contingency Planning Group. More information on the National Contingency Planning Group can be found under **National Emergency Preparedness** (see paragraph 25.74).

25.33 Using a common checklist, the Secretariat and the National Contingency Planning Group reviewed for completeness the plans submitted by the

23 organizations and the approval structures to be used in executing the plans.

We brought our findings to management's attention in the organizations that we audited and encouraged each to take further action.

25.34 Our review of contingency plans of the six organizations noted that some of the required components were missing and that some components contained only broadly defined information.

25.35 A common finding was that the test plans were incomplete. Most organizations did not plan to test components of their contingency plans before the start of the validation exercise that was developed by the National Contingency Planning Group. Some planned to rely primarily on that exercise in order to test their contingency procedures. The validation exercise was developed to test the government's capacity for co-ordinating a response to several concurrent emergencies and to give organizations an opportunity to test their contingency plans. It was not designed to test contingency procedures for all mission-critical systems and processes in an organization. The testing that the exercise provided may not be sufficient for all organizations.

25.36 We brought our findings to management's attention in the organizations that we audited and encouraged each to complete the contingency plans expeditiously and to test critical contingency procedures in its plans, particularly in areas of higher vulnerability. Several management responses indicated that testing, over and above the validation exercise, was planned or contemplated for November. One department advised us that it had completed many aspects of its test plan before the start of the validation exercise.

The two regulatory agencies used a risk-based strategy to assess the impact of Year 2000 on those they license.

Regulatory Responsibilities

25.37 As a regulator, the government has the responsibility to ensure that the industries it regulates continue to meet regulatory requirements, notwithstanding the Year 2000 computer problem. As previously noted, we examined two areas that are regulated by the government — medical devices at Health Canada and nuclear facilities and radioactive devices at the Atomic Energy Control Board.

25.38 The Board regulates the ongoing operations and the operators of nuclear facilities and radioactive devices. Health Canada licenses new medical devices and establishments that manufacture, import and distribute medical devices. We would expect each of the regulatory agencies to assess risks arising from Year 2000 in order to determine if further regulatory requirements would be appropriate. We would also expect them to prioritize their compliance and enforcement activities on the basis of their risk assessments.

Additional requirements were set for nuclear power reactors, higher-risk radioactive devices and medical devices

25.39 The two regulatory agencies used a risk-based strategy to assess the impact of Year 2000 on those they license. Both had prepared legal assessments, including recommendations and suggestions for action. The agencies have determined that no amendments to regulations are required in their respective areas.

25.40 Three of approximately 100 licensees of nuclear facilities are responsible for all operating nuclear power reactors in Canada. The Atomic Energy Control Board wrote to the three licensees to require that by 1 October 1998, all special safety systems — those that provide for the safe shutdown of a nuclear power reactor — be corrected, tested and made compliant for Year 2000. The systems whose failure could trigger the special safety systems were to be compliant by 31 December 1998. Finally, by 30 June 1999 the three licensees were to provide assurance to the Board that all systems were ready for continued operation into 2000, with no undue risk to health, safety, security and the environment.

25.41 The Board developed a risk profile and criteria to assess over 3,700 licensees of radioactive devices for radiological risk in the transition to 2000. A total of 443 licensees met the profile and the criteria and were thus selected to demonstrate readiness for Year 2000. Those licensees were required to respond by 31 October 1998 to a questionnaire on the status of their Year 2000 programs. By 31 March 1999, they were to submit their plans for mitigating any Year 2000 problems that could compromise the safety of their activities. Confirmation that all problems related to Year 2000 had been identified and corrected was required by 30 June 1999.

25.42 At Health Canada, the Health Protection Branch contacted about 2,040 licensed manufacturers and suppliers of medical devices to remind them of Year 2000 risks and their responsibilities under the Medical Devices Regulations of the *Food and Drugs Act*. It requested that the licensees test all devices that were still in use and report to the Branch by 30 May 1998 on the status of compliance for Year 2000. In addition, the Branch requested information on test results to support the compliance status reported. In June 1999, the Branch advised the licensees that annual licence renewal, required by 1 November, would take place only if licensees attested that date-sensitive devices were compliant for Year 2000.

Many licensees reported compliance for Year 2000 but some follow-up is still required

25.43 The licensees for nuclear power reactors have met all deadlines. We found that the Atomic Energy Control Board has addressed Year 2000 risks and exposure in its monitoring and enforcement activities for nuclear power reactors. Licensees had to demonstrate to Board inspectors that safe operations would be maintained throughout the period of the transition from 1999 to 2000. In addition, licensees were required to demonstrate that they have contingency plans in place to accommodate any risks that are beyond their control, such as loss of electrical power and problems in the transportation and communications sectors.

The licensees for nuclear power reactors have met all deadlines.

25.44 With respect to the radioactive devices identified as higher-risk, about 90 licensees or one fifth of the identified group had not responded by July 1999. In total, we found that some 29 percent had yet to demonstrate that they had met the requirement to identify and rectify all Year 2000 issues by 30 June 1999 (see Exhibit 25.3). In September 1999, we reported this finding directly to the Atomic Energy Control Board and suggested that it follow up with delinquent licensees and escalate its action as appropriate. The Board acknowledged our findings and suggestions and agreed to take them into account in its remaining activities in 1999. In late September, it advised us that cases involving 13 percent of the licensees remained unresolved.

25.45 Using the information on Year 2000 compliance that it received from licensed manufacturers of medical devices, the Health Protection Branch of Health Canada constructed a database and made it available on the Branch's Web site. Although this is not part of the Branch's regular activities, the database provides a wealth of information for health care professionals and institutions. For the health care sector, compliance information is important on all devices that are in use, not just those that continue to be manufactured.

25.46 The devices are classified into four risk classes according to the Medical Devices Regulations of the *Food and Drugs Act.* Class IV devices are those with the highest risk to the human body and Class I are those with the lowest risk. For example, Class IV devices include implanted cardiac pacemakers and other life support systems; Class III devices include X-ray machines and certain types of resuscitators.

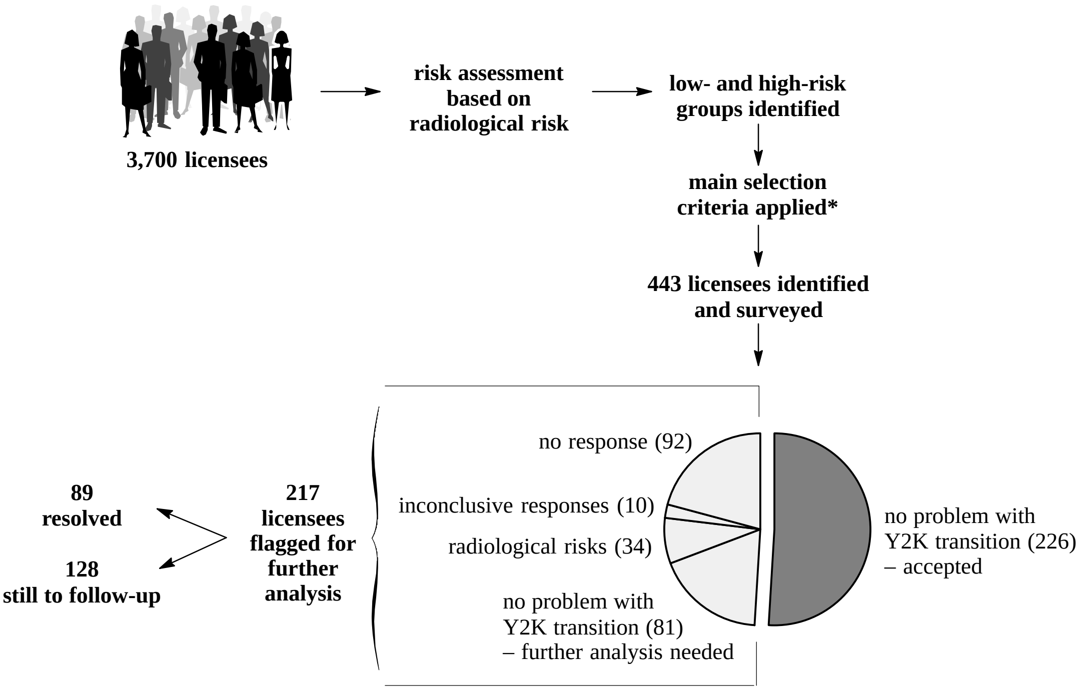
25.47 After receiving information from licensees, the Health Protection Branch categorized their responses by status of compliance for Year 2000. According to information in the database, licensed manufacturers of all Class IV devices and over 75 percent of those of Class III devices have responded and provided compliance information. Exhibit 25.4 shows the status of the database at September 1999.

25.48 We conducted a sample check of about 48 devices on the database and compared compliance information on the Department's Web site with its documents and files or the manufacturer's Web site. We found several cases where, in our view, further follow-up was appropriate. For example, several Class IV devices were recorded as compliance category 5 (device no longer sold, company does not have compliance information). Users of those devices have no compliance information from Health Canada.

25.49 We reported the detailed findings of our sample check to the Department and suggested that it consider further follow-up with licensed manufacturers to make the database more useful to health care users. We also suggested that the Department consider the merits of further reviewing its database and following up on other delinquent licensees. In

Exhibit 25.3

Status of Responses From Licensees of Radioactive Devices Identified as Higher-Risk


3,700 licensees
risk assessment based on radiological risk
low- and high-risk groups identified
main selection criteria applied*
443 licensees identified and surveyed
no response (92)
inconclusive responses (10)
radiological risks (34)
no problem with Y2K transition (81) – further analysis needed
no problem with Y2K transition (226) – accepted
217 licensees flagged for further analysis
89 resolved
128 still to follow-up

* **Main Selection Criteria**

- Size of source of radiation
- Likelihood of exposure
- Potential to hit or exceed a targeted level of safety
- Level of automation of processes
- Complexity of the licensed activity
- Ability to modify equipment to make it Y2K vulnerable
- Degree of regulatory control and oversight

Source: Examinations of internal documents and interviews with project officials, July 1999 mid-September, the Department advised us that it would look at the specific gaps we had noted in its database.

Other Government-Wide Issues

25.50 In our two previous audits, we identified several areas where departments have common needs and where efficiencies could be gained by addressing common issues horizontally. In the current audit, we followed up on three specific horizontal issues and the Treasury Board Secretariat's response to our recommendation that government reporting to Parliament on Year 2000 progress be improved.

Review of departmental contingency plans

25.51 The development of contingency plans was a key activity for organizations in 1999. The Secretariat identified the need to oversee the development of contingency plans in the 23 departments, agencies and Crown corporations that are responsible for government-wide mission-critical functions.

25.52 We note that the Secretariat has issued guidelines to assist individual departments in preparing contingency plans. In addition, it has held workshops and information sessions in co-operation with the National Contingency Planning Group to explain the guidelines.

25.53 According to targets set by the Treasury Board Secretariat and the National Contingency Planning Group, all components of the 23 sets of departmental contingency plans were to be completed by April 1999. In addition to risk analysis and a contingency plan overview, the components also include plans and procedures for crisis response, business resumption, training and testing.

25.54 During the audit, we reviewed the contingency plans of eight departments and agencies and noted that some key deliverables either had not been submitted or were broadly written documents with few details. For example, in June 1999 the Secretariat had not received from five of the eight departments their completed plans and procedures for crisis response and business resumption. We followed up on the updates prepared by the six departments we audited for GWMC functions. Most of them had completed the crisis response portion of the plans; two departments needed to complete additional details for business resumption.

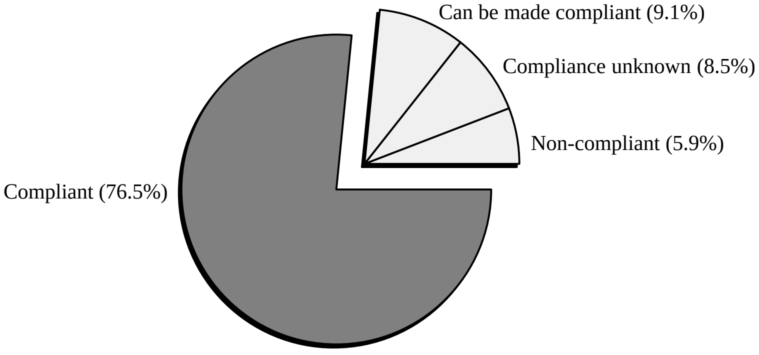
25.55 The Secretariat has developed a checklist as a tool to oversee the completeness of contingency planning documents at departments and agencies. We noted that for some key deliverables, the Secretariat would consider that the organization had met the requirements if it had:

- completed the procedures; or
- provided a workplan for their completion; or
- stated in writing that further work was not necessary.

25.56 We suggested to the Secretariat in its oversight role that before accepting contingency plans as complete, it seek

Exhibit 25.4

Status of Health Canada's Database on Year 2000 Compliance of Medical Devices



Source: Health Canada, September 1999 additional information from the department or agency to satisfy itself that the key deliverables could be completed in time or that no further work was needed. The Secretariat advised us that its first-phase checklist focussed on the robustness of the contingency planning regime and that it has developed a checklist for a second phase to monitor the finalization of the plans. The Secretariat indicated that it was in the process of implementing this second phase of monitoring.

Government-wide communications strategy for Year 2000

The government has been providing up-to-date information related to Year 2000 on its Web sites.

25.57 The need for a communications strategy for the government as a whole was also identified as a key activity for 1999. From a government perspective, there needs to be a consistent and coherent approach to providing Year 2000 information to stakeholders and the public. From a public perspective, there is a need to be kept informed about the government's readiness so that individuals and organizations can make their own plans in advance of January 2000.

25.58 Working with key departments and the Privy Council Office, the Secretariat has developed a government-wide communications strategy. Its stated objective is:

> To provide relevant, timely and credible information to all publics in a proactive manner on the action taken by government departments and its provincial/territorial and private sector partners, in order to build and maintain public confidence and to encourage preparedness for the Year 2000 transition.

Overall funding of $1.5 million has been approved for Year 2000-related communications over a period of about 18 months ending in March 2000.

25.59 We found the strategy to be comprehensive. It covers three key audiences — inside the government, external domestic and external international. It also has a list of key messages to be communicated. One is that the government's overall priority is making sure that the systems essential to the health, safety, security and economic well-being of Canadians are compliant for Year 2000 and providing leadership to encourage Canadians to meet the Year 2000 challenge.

25.60 The strategy considered the need to provide Canadians with timely, factual and useful information throughout 1999. It emphasized the need for the government to be transparent about its state of preparedness for delivering essential services and to be accurate in providing third-party information. Where third-party information has not been verified, the government intends to clearly state that fact.

25.61 At September 1999, we noted that the government had prepared and sent Year 2000 information flyers to Canadian households. It has held a number of events to communicate not only its own Year 2000 progress but also the state of preparedness of key industries and utilities such as banking, hydroelectricity and telecommunications services. Moreover, the government has been providing up-to-date information related to Year 2000 on its Web sites and through its toll-free telephone enquiry service.

Funding for Year 2000 projects

25.62 In 1997, we identified the issue of funding for Year 2000 as a risk that could delay Year 2000 readiness. In 1998, we noted that the Secretariat had established a mechanism to loan funds to the 23 departments, agencies and Crown corporations that are responsible for government-wide mission-critical functions. By July 1998, $365 million of a $400 million budget had been loaned.

25.63 In 1999, additional submissions have been made to the Treasury Board for Year 2000 loan funding. By 25 August

1999, approved loans had risen to $723 million. Nineteen departments, agencies and Crown corporations requested a total of $592 million in Year 2000 loan funding for GWMC functions. Seven of those organizations also requested loan funds for their department-wide mission-critical functions. In addition, five organizations that are not responsible for GWMC functions requested loan funds for Year 2000 projects to prepare their department-wide mission-critical functions. Loans for department-wide mission-critical functions totalled $131 million.

25.64 We note that the standard term for repayment is three years commencing in 2001–02 but that it can be reviewed, depending on affordability, where the ability to deliver programs is at risk.

25.65 Given the magnitude of Year 2000 projects and their immovable deadlines, many organizations have put other development projects on hold and kept systems maintenance to a minimum. The 24 departments and agencies that received Year 2000 funds will be faced with balancing additional demand for new information technology projects while repaying their loans. Furthermore, departments and agencies are planning to implement a common information management and information technology infrastructure and other systems changes to support electronic service delivery. In our view, the Secretariat needs to ensure that the loan repayment takes into account the ability of departments and agencies to support electronic service delivery.

In our view, the Secretariat needs to ensure that the loan repayment takes into account the ability of departments and agencies to support electronic service delivery.

Managing transition to Year 2000

25.66 The "transition period" for Year 2000 is the period around 1 January 2000, when special measures may have to be introduced to monitor and resolve any problems that may arise.

25.67 In March 1999, the Secretariat and departments discussed the concept of transition management and the need for a co-ordinated approach to this rollover period. A Transition Study Group was formed, with 10 departments participating. In June 1999, the Group completed a guideline entitled "The Year 2000 Transition of Production Information Systems". This Treasury Board Secretariat guideline was intended to assist departments and agencies in planning for transition management in their own entities.

25.68 Together with departments and agencies, the Secretariat has a role in co-ordinating and managing the Year 2000 transition for all GWMC functions.

25.69 Departments and agencies have been setting their own rollover periods for managing the transition. The Year 2000 Project Office at the Secretariat has been referring informally to the period from 15 December 1999 to 15 January 2000 as the likely period for co-ordinating and managing the Year 2000 transition, but this has not been formalized. By early September 1999, few details had been determined on how multiple problems in different GWMC functions would be co-ordinated and managed at a government-wide level.

25.70 We suggested to the Secretariat that it expedite planning to co-ordinate and manage the Year 2000 transition on a government-wide level; consider setting a time frame as the government-wide rollover period for Year 2000; and determine the respective roles and responsibilities of various parties, including the National Contingency Planning Group (NCPG). The Secretariat has advised us that it has had discussions with the NCPG to clarify its role for government-wide mission-critical functions.

Reporting to Parliament

25.71 In its response to our 1998 recommendation calling for improved reporting to Parliament, the Treasury Board Secretariat indicated that it would continue to examine ways of keeping Parliament informed.

25.72 It has done this through the House of Commons standing committees on Industry and on Public Accounts. In 1997 and 1998, the Secretariat provided testimony to the Industry Committee on the government's Year 2000 progress. A number of departments also provided testimony to that Committee. To the Public Accounts Committee, in addition to providing testimony in several hearings in 1997 and 1998, the Secretariat submitted two progress reports in 1998. Since January 1999, it has provided monthly reports to the Public Accounts Committee. The 26 August report on the status of progress at July 1999 was the last in that series.

25.73 In the current audit, we found that the Secretariat had improved the format and content of its Year 2000 progress reporting to the Public Accounts Committee. Instead of reporting the progress made in each organization, it provided information on progress in each of the 43 government-wide mission-critical functions. In almost all cases, progress in department-wide mission-critical functions for the 23 departments, agencies and Crown corporations was included in those reports.

National Emergency Preparedness

A formal group was set up to co-ordinate the development of national contingency plans

The government also gives priority to the possible need for responding to major disruptions in Canada or to a series of smaller incidents in several locations as a result of the Year 2000 computer problem.

25.74 As we have noted, planning for Year 2000 contingencies is prudent and essential to ensure that critical functions continue. Although high priority is given to plans and procedures for working around systems that support government-wide mission-critical functions, the government also gives priority to the possible need for responding to major disruptions in Canada or to a series of smaller incidents in several locations as a result of the Year 2000 computer problem.

25.75 National Defence was given the responsibility to lead and co-ordinate these efforts. In October 1998, a federal official was appointed to co-ordinate and facilitate the development of national contingency plans for Year 2000. The group that he leads, the National Contingency Planning Group (NCPG), comprises a dedicated staff of about 80 people, mostly on assignment from various departments and agencies. As part of this national support initiative, the operations of Emergency Preparedness Canada have been integrated into those of the NCPG but for Year 2000 activities only. Operation Abacus was set up separately at National Defence to prepare the Canadian Forces to respond to requests from civil authorities for assistance.

25.76 The NCPG conducts and co-ordinates a number of concurrent events. Exhibit 25.5 provides a simplified view of its key activities. One major milestone was the identification of elements of critical national infrastructure, such as transportation and utilities, and assessment of the risk of their potential Year 2000 failure. Another key activity was the development of a national validation exercise planned for the end of September 1999. Starting in October 1999, the NCPG planned to shift its focus to transition period activities, like co-ordinating available Year 2000 information within government for the appropriate authorities.

Many tasks were accomplished, including preparing for the validation exercise

25.77 In February 1999, the Group finished identifying and defining elements of Canada's critical infrastructure. We noted that its national infrastructure risk assessment (NIRA) is a detailed bimonthly assessment by element, based on two factors — the criticality of the infrastructure element and the likelihood of Year 2000 failure.

25.78 The assessment of criticality was based on information the NCPG collected from a broad group of stakeholders, including key industries and other levels of government. It assessed the likelihood of Year 2000 failure on the basis of the state of preparedness for Year 2000 and progress in developing contingency plans. The interdependencies identified in those plans were used in assessing the potential impact of failure of critical infrastructure elements.

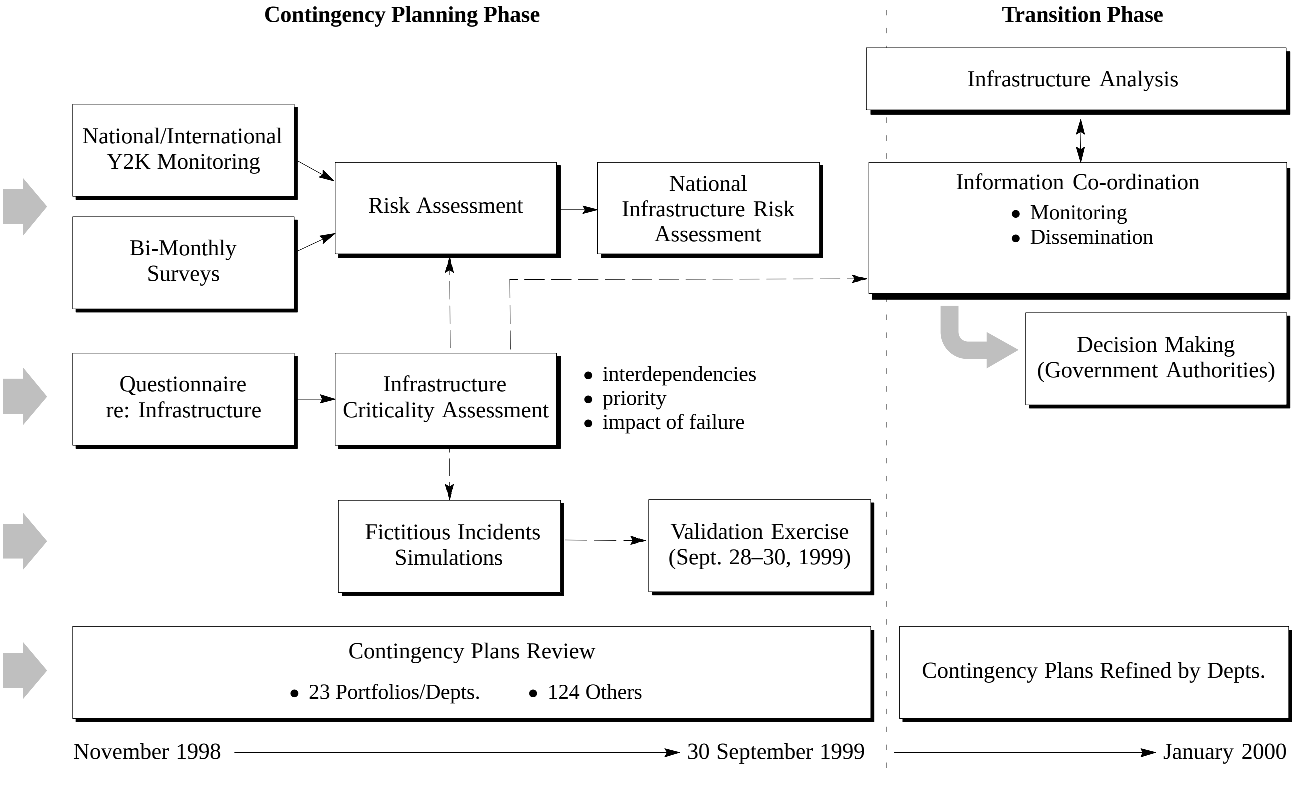
25.79 We reviewed two elements of one NIRA and noted that the assessments were thorough and complete. At early September 1999, the NCPG had completed three NIRAs. It planned to complete three additional assessments, the last by mid-December 1999.

25.80 Using the assessment of criticality, the NCPG formulated fictitious incidents for the three-day NCPG validation exercise. The purpose of the exercise was to evaluate the government's capacity to co-ordinate a response to several concurrent emergencies, and to provide an opportunity for organizations to test their contingency plans. All 23 mission-critical departments, agencies and Crown corporations were required to participate in that exercise; participation by other organizations was voluntary. The validation exercise was held at the end of September 1999. The NCPG has advised us that the exercise proved to be very

The National Contingency Planning Group has advised us that the validation exercise proved to be very useful.

Exhibit 25.5

Key Activities of the National Contingency Planning Group


Contingency Planning Phase
Transition Phase
National/International Y2K Monitoring
Bi-Monthly Surveys
Risk Assessment
National Infrastructure Risk Assessment
Infrastructure Analysis
Information Co-ordination
• Monitoring
• Dissemination
Decision Making (Government Authorities)
Questionnaire re: Infrastructure
Infrastructure Criticality Assessment
• interdependencies
• priority
• impact of failure
Fictitious Incidents Simulations
Validation Exercise (Sept. 28–30, 1999)
Contingency Plans Review
• 23 Portfolios/Depts.
• 124 Others
Contingency Plans Refined by Depts.
November 1998
30 September 1999
January 2000

Source: Simplified and adapted from various documents of the National Contingency Planning Group useful and that several companies from industry also participated. It indicated that various organizations were analyzing the results to improve their plans, particularly the way information was to be analyzed and communicated during an incident.

25.81 The National Contingency Planning Group also played an important role in reviewing the contingency plans of government departments and agencies. By 30 April 1999, the 23 departments and agencies that are responsible for government-wide mission-critical functions were to complete various components of their contingency plans and submit them to the Treasury Board Secretariat and the NCPG for review. Moreover, using the same target dates, the NCPG called for the submission of contingency plans from 124 other departments and agencies. In total, 147 organizations were expected to submit their contingency plans to the NCPG for review.

25.82 We found at 10 September 1999 that 50 of the 147 organizations had not completed contingency plans to meet all requirements that had been set for April 1999. In addition, 6 organizations had not filed any contingency plans. We also noted a general tendency of departments and agencies to rely primarily on the NCPG validation exercise to test their contingency plans. This was partly the purpose of that exercise, but it was not designed to challenge all significant operations of an individual department.

25.83 We communicated our findings to the NCPG in September 1999 and suggested that it follow up further on delinquent departments and agencies and those that had not completed their contingency plans. We also suggested that the NCPG continue to encourage the organizations to complement the validation exercise with their own testing.

Measures were being put in place to respond to possible requests for emergency assistance

25.84 Emergency Preparedness Canada is one of several important players on an integrated transition team of the government for co-ordinating federal responses to Year 2000 disruptions. It has reorganized its National Support Centre, ordinarily used for isolated major emergency events to collect, analyze and disseminate information on Year 2000 events from around the country and internationally and to support the co-ordination of federal responses.

25.85 In August 1999, senior analyst support for operations was available only during regular hours. Over the fall of 1999, Emergency Preparedness Canada expected to fully staff three shifts to allow for comprehensive support on a 24-hour, seven-days-a-week basis. As we concluded our audit, the Secretariat and the NCPG were clarifying their respective roles.

25.86 In preparing to respond to possible requests for assistance as a result of Year 2000 disruptions, National Defence had modified the leave policy for its forces between 15 November 1999 and 31 March 2000. In August 1998, Operation Abacus was initiated to prepare the Canadian Forces. Most of the efforts in the past 12 months have involved planning for a number of essential activities, such as assessing potential demands for assistance and training Canadian Forces personnel.

National Defence planned to put in place its command and control structure after 30 November 1999 and to be on standby for potential requests for assistance across Canada starting 31 December 1999.

25.87 As of mid-September 1999, National Defence had released to its staff the final draft of the Operation Abacus operating instructions. It was completing its planned training exercises and preparing to participate in the NCPG validation exercise, with a focus on elements of command, control and communications. It planned to put in place its command and control structure after 30 November 1999 and to be on standby for potential requests for assistance across Canada starting 31 December 1999. National Defence anticipated that its forces would remain on call for 30 days or longer as needed, following the last week of December 1999. Its command, control, communications and liaison structure would remain in place until the end of March 2000 if necessary.

Looking Beyond Year 2000

25.88 Reflecting upon this $2 billion Year 2000 project, we observed several issues that are worthy of consideration for action beyond December 1999.

Government date standards need to be observed

25.89 Information technology standards for departments and agencies are set by the Treasury Board through its Treasury Board Information Technology (TBIT) standards program. As we noted in the follow-up to our September 1996 Report Chapter 16 (see Chapter 32 of this Report, paragraph 32.26), the TBIT standards program has remained largely at the policy level and, to date, has not been implemented by departments and agencies.

25.90 The TBIT standards for date coding were set as far back as 1988. In TBIT standard–36, “all-numeric representation of dates and times”, the standard requires an eight-digit date code for a calendar date, in three elements in the order of year-month-day (seven digits for a Julian date, in the order of year-day of year). Had the TBIT date standard been observed in the past, the scope and extent of the government’s Year 2000 work would have been greatly reduced.

25.91 In considering a Year 2000 remediation strategy, many organizations in both private and public sectors turned to a “windowing” technique instead of expanding the two-digit year code to four. That strategy is more efficient and can reduce the potential for introducing errors into application systems through date expansion.

25.92 In the government, each department and agency determined its own remediation strategy for Year 2000. From the Year 2000 audits we conducted, we noted that both date expansion and windowing remediation strategies were used. Moreover, in the departments and agencies we reviewed (nine in 1997 and six in 1998, three of which had also been examined in 1997), none of the remediation strategies referred to the TBIT standards or to a migration plan in the future to meet those date standards.

25.93 The windowing technique requires ongoing maintenance to ensure that systems interpret the year properly. For example, the repaired Canada Pension Plan system will be able to recognize years up to and including 2065; changes will have to be made to the system before it can accept years beyond that year. We noted that some departments have department-wide date standards, but this is not a standing feature in all departments and agencies. Standardized representation of a data element as ubiquitous as the date would foster interoperability among departments and support the government’s agenda to integrate services in order to better serve the public. In our view, the TBIT date standards need to be observed.

Had the Treasury Board Information Technology date standard been observed in the past, the scope and extent of the government’s Year 2000 work would have been greatly reduced.

25.94 **The Treasury Board Secretariat should ensure that all departments and agencies are made aware of the existing government date standards and that departmental plans are in place to comply with them in future upgrades and maintenance of departmental systems.**

Government’s response: *The Year 2000 issue has increased awareness of the Treasury Board Information Technology date standard, and the importance of standards in general. As part of the Year 2000 close-down procedures, the Secretariat will issue a memorandum to departments reminding them of the date standard and urging that it be* *implemented when amending existing, or developing new, date processing logic.*

Once the government has successfully transitioned from Year 2000 activities, the Chief Information Officer Branch of the Secretariat will undertake a review of the status of departments' use of date formats and windowing techniques to determine the need for further direction and guidance.

Opportunity to harness Year 2000 legacy

25.95 The Year 2000 computer problem provided an opportunity for organizations to better understand not only their dependence on information technology but also their interdependence with partners and stakeholders. Moreover, Year 2000 projects provided an impetus for organizations to thoroughly document their information systems and devices and determine their criticality to the organizations.

25.96 As never before, contingency planning became a key activity. Staff in information technology and business units worked together to make major decisions such as identifying mission-critical activities, determining minimum acceptable levels of service and developing contingency procedures for maintaining them.

25.97 Information technology changes at a rapid pace. The government's move to electronic service delivery will also change service channels and procedures. Without regular updates, systems inventories and contingency plans will soon be out-of-date. Information bases such as systems inventories and contingency plans are a Year 2000 legacy that ought to be valued and maintained.

25.98 The Treasury Board Secretariat should consider requiring departments and agencies to maintain and update valuable information bases, such as systems inventories and contingency plans, that were developed to respond to Year 2000.

Government's response: *The Year 2000 Project Office of the Secretariat has established an interdepartmental committee to identify, recommend and support Year 2000 project completion activities. A key objective of the work of this committee will be to help ensure that the products and benefits of the project are preserved and exploited.*

Need for vigilance over potential Year 2000 pitfalls

Year 2000 could continue to plague systems and operations beyond 1 January 2000.

25.99 From discussion with analysts in the information technology industry and a review of related articles, we noted that Year 2000 could continue to plague systems and operations beyond 1 January 2000. Some have identified 1 March 2000, the first day after 29 February, the leap year date, as a problem date that could equal 1 January 2000 in its impact. Others noted that problems could continue well into 2000.

25.100 An example of such problems is the risk of data corruption. Incorrect data could be introduced through undetected errors in an application system. Further, the more a system interfaces externally with other systems, the higher its exposure to the risk that data could be tainted by non-compliant data sources or by misinterpretation of incoming data.

25.101 Another example is the risk that archived data will be inaccessible. As systems have been repaired or replaced, not all organizations have paid due regard to the data that they have archived. There is a risk that new systems will not be able to access archived data and, since the old systems are not Year 2000 compliant, they cannot be used beyond 1999.

25.102 In our view, the government needs to remain vigilant beyond 1999 and keep watch over potential Year 2000 pitfalls.

25.103 The government should ensure that departments and agencies have

procedures in place to guard against potential Year 2000 pitfalls after January 2000.

Government's response: *In recognition of the continued threat of Year 2000 problems past 1 January 2000, the government plans to continue to dedicate resources to the issue into the new year. The Year 2000 Project Office of the Secretariat will maintain existing staffing levels until 31 March 2000. Provisions have been made to continue an office at reduced levels throughout the 2000–2001 fiscal year. The list of dangerous dates published to departments and agencies included 29 February 2000 of the leap year.*

We expect that the interdepartmental project completion committee, mentioned in the response to paragraph 25.98, will also identify ongoing measures that should be put in place to offset potential Year 2000 threats.

Conclusion

25.104 We set out to assess the government's progress in preparing its government-wide mission-critical functions for Year 2000; its activities to discharge its regulatory responsibilities in the face of Year 2000 risks; and its efforts to prepare for national emergencies that may arise after December 1999.

25.105 In August 1999, the Secretariat reported that systems supporting government-wide mission-critical functions had achieved an overall completion rate of 99 percent at July 1999. Organizations with those systems that required additional testing and full implementation were planning to complete them in September and October 1999. We concluded that the government has made significant progress since our audit in 1998.

25.106 We noted that departments and agencies have made major efforts to develop contingency plans. In the departmental contingency plans we reviewed, contingency procedures had largely been defined but some components were not complete, and few departments had developed test plans when we completed our audit in early September.

25.107 We found that Year 2000 requirements had been established for licensees of nuclear power reactors and radioactive devices as well as medical devices. Although we observed a need for some follow-up, the licensees for active nuclear power plants had met all regulatory requirements to prepare for Year 2000; compliance information on medical devices had been requested and made available to health care professionals and institutions.

25.108 In preparing for a national emergency, the National Contingency Planning Group identified elements of critical national infrastructure and assessed the risks presented by Year 2000. The Group also developed a validation exercise and set up an information and response co-ordination centre. Operation Abacus in National Defence was establishing a structure to support any emergency assistance that may be required in 2000.

25.109 As we completed our audit in September 1999, much had been accomplished in the areas we audited. Nevertheless, some Year 2000 work programs still have to be completed and the government needs to remain vigilant to minimize any Year 2000 disruptions.

About the Audit

Objectives

The 1999 audit focussed on the government’s final preparation for the Year 2000 computer problem. The objectives of the audit were to assess:

- the progress that the government has made in this final year in remediating and testing systems that support government-wide mission-critical functions and in implementing them;
- government efforts to provide for national contingencies and emergencies; and
- Year 2000 activities for discharging regulatory responsibilities.

Scope

We reviewed Year 2000 progress reports prepared by the Treasury Board Secretariat, and the supporting files. For seven mission-critical functions, we also examined results of remediation and testing at the responsible department or Crown corporation. Those functions and the six organizations responsible for them are as follows:

- emergency broadcasting (Canadian Broadcasting Corporation);
- weather forecasting (Environment Canada);
- export and import controls (Foreign Affairs and International Trade);
- income security (Human Resources Development Canada);
- employment insurance (Human Resources Development Canada);
- Receiver General (Public Works and Government Services Canada); and
- income tax processing (Revenue Canada).

We also examined several horizontal issues managed and overseen by the Secretariat, such as the government’s communications strategy and departmental contingency planning.

For national emergency preparedness, we interviewed staff and examined files of the National Contingency Planning Group and Operation Abacus at National Defence. We selected two regulatory functions that can impact public health and safety — medical devices regulated by Health Canada and nuclear facilities and radioactive devices regulated by the Atomic Energy Control Board.

The government assigned additional Year 2000 responsibilities to four departments and agencies — Treasury Board Secretariat for monitoring government readiness; Industry Canada for preparing the private sector; Foreign Affairs and International Trade for monitoring international activities; and National Defence for responding to national emergencies. The audit did not extend to those activities under Industry Canada or Foreign Affairs and International Trade.

In addition to systems that support government-wide mission-critical functions, departments and agencies have systems that are critical to their own operations. We did not audit those departmental mission-critical systems.

The audit was not designed to and did not provide assurance that the government will be able to deliver all government-wide mission-critical functions in 2000. It did not provide assurance that, relative to Year 2000, adequate steps had been taken by the regulatory agencies for areas they regulate or that the government will be ready to respond to national emergencies.

The government remains responsible for its systems and their ability to continue to function properly beyond 1999. Its regulatory agencies are responsible for discharging their responsibilities relating to Year 2000 and it remains a government responsibility to be able to respond to national emergencies.

Criteria

Where appropriate, detailed criteria are discussed in sections containing our observations and findings. The general criteria for the audit were as follows:

Government preparedness

- Departments and agencies should conduct Year 2000 work on systems supporting critical functions in accordance with departmental plans and target completion dates set out by the Treasury Board Secretariat, to ensure that compliant systems for critical functions are successfully implemented before 2000.
- Departmental Year 2000 project management offices should provide sufficient, appropriate and timely progress information to senior management and the Secretariat on a regular basis.
- The Treasury Board Secretariat should monitor monthly Year 2000 progress on government-wide mission-critical systems at departments and agencies. Strategic intervention should be exercised as appropriate.
- For all critical functions, contingency plans and business resumption plans should be prepared and tested and, where warranted, be put in place before 2000.
- The Treasury Board Secretariat should co-ordinate and facilitate departmental Year 2000 efforts on common issues, including a Year 2000 communication strategy, to expedite progress and maximize cost effectiveness. Where appropriate, the Secretariat should provide guidance to assist departments and agencies in their Year 2000 work.
- Parliament should be kept informed of matters of significance arising from the Year 2000 challenge and its effects on government operations and service delivery.

National emergency preparedness

- The National Contingency Planning Group should :
  - identify potential risks to Canada’s critical national infrastructure arising from possible Year 2000 disruptions, based on information provided by responsible organizations; and

- co-ordinate the development of contingency plans at the national level by facilitating, through responsible departments and agencies, the participation of those sectors comprising Canada's critical infrastructure.

- Measures should be put in place to prepare for potential Year 2000 disruptions of the national infrastructure and to respond to them should federal assistance be requested or required.

Regulatory agencies

- As part of its regulatory responsibilities over licensees, the agency should identify risks associated with potential Year 2000 disruptions and set out regulatory requirements as appropriate to ensure that its responsibilities are properly discharged.

- The agency should prioritize its enforcement activities based on Year 2000 risk assessments of its licensees to minimize the impact on public health and safety. Consideration should also be given to results of legal analysis and assessment.

Audit Team

Assistant Auditor General: Doug Timmins
Principal: Nancy Cheng
Directors: Maria Wisniowski, Greg Boyd, Tony Brigandi and Guy Dumas

Joe Lajeunesse
Peter Taylor

For additional information, please contact Nancy Cheng.