Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 26-Aug-1998
Dist. : 27-Aug-1998

Or. Eng.

PUMA(98)10
Unclassified

PUBLIC MANAGEMENT SERVICE
PUBLIC MANAGEMENT COMMITTEE

THE YEAR 2000: IMPACTS AND ACTIONS

This draft report has been developed in response to a request at the 1998 Council meeting at Ministerial level that the OECD "promote global awareness of the Year 2000 problem and its potential economic impact," and report to the Ottawa ministerial conference on electronic commerce that will be held 5-7 October. The PUMA-co-ordinated report includes a review of economy-wide and sectoral impacts carried out by the Directorate for Science, Technology and Industry, as well as a PUMA-written chapter on governments' role and actions, based primarily on responses to a PUMA questionnaire received from countries in June and July.

Before providing the report to the OECD Council in September and delivering it to Ottawa, the PUMA Committee and country Year 2000 contacts are requested to provide written comments to the PUMA Secretariat by 7 September, 1998.

68433

Or. Eng.

PUMA(98)10

THE YEAR 2000 PROBLEM: IMPACTS AND ACTIONS

1. This draft report has been developed in response to a request at the 1998 Council meeting at Ministerial level that the OECD "promote global awareness of the Year 2000 problem and its potential economic impact," and report to the Ottawa ministerial conference on electronic commerce that will be held 5-7 October. The PUMA-co-ordinated report includes a review of economy-wide and sectoral impacts carried out by the Directorate for Science, Technology and Industry, as well as a PUMA-written chapter on governments' role and actions, based primarily on responses to a PUMA questionnaire received from countries in June and July.

2. Before providing the report to the OECD Council in September and delivering it to Ottawa, the PUMA Committee and country Year 2000 contacts are requested to **provide written comments to the PUMA Secretariat by 7 September, 1998.** Comments should be sent to Daniel Blume (Daniel.Blume@oecd.org; telephone 33.1.45.24.97.59; fax 33.1.45.24.87.96).

3. The report generally is only as up to date as the responses provided to the questionnaire, and therefore any suggested language to update or clarify information on the situation in each country would be particularly appreciated. Although it is recognized that the two weeks provided for comment is tight, the comment period is limited by the need to provide adequate time for OECD Council review prior to the Ministerial meeting in Ottawa.

4. Once comments are taken into account, it is intended to publish the report under the authority of the Secretary-General and also to distribute it to the "Global Year 2000 Summit," to be held in London 15-16 October. This meeting is being organised by the World Information Technology and Services Alliance (WITSA) in collaboration with the OECD and other international and private sector organisations. Documentation on this is meeting is available on the OECD's On Line Information System (OLIS) [PUMA(98)9], and regularly updated information on the programme is also available at http://www.itaa.org/globaly2k.htm.

EXECUTIVE SUMMARY

1. The so-called “Millennium bug” places at risk information networks and electronic systems that have become pervasive throughout the OECD and much of the world. This report aims to support countries in responding to this potential threat to global economic and citizen well-being by providing information on the nature and extent of the problem, its economy-wide impacts, and the initiatives being taken at both a national and international level to address it.

In brief, the report concludes:

- **While awareness is increasing, the amount of remediation still required is daunting.** The problem continues to be under-estimated, and full-scale actions to address it are only recently beginning in many countries. Preparedness among the health care industry, small businesses and some parts of government appears to be particularly worrisome;
- **Significant negative economic impacts are likely in the short-term**, though there is much uncertainty regarding the extent of disruptions that the Year 2000 problem will cause;
- **Governments face a major public management challenge, requiring acceleration of their own preparations and a stronger leadership role** to increase awareness and understanding of the problem, and to promote action to address it economy-wide.
- **Stronger international co-operation is essential**, particularly in relation to cross-border testing, given global economic interdependence and the particular interconnections in such areas as energy, telecommunications, transport and international financial transactions.

2. The Year 2000 problem, also referred to as “Y2K,” stems from early programmers’ need to save memory in writing software or chip design. Without conversion, many existing systems will not recognise "00" as "2000", but as “1900” (or as an invalid date). Problems may arise not only in computer systems, but also in communication networks and in chips integrated into industrial control systems, consumer electronic devices and safety systems. Although the failure rate of such “embedded systems” is very low (experts estimate a 1% to 3% range), the sheer number of such hidden devices presents a significant challenge (the number of installed chips is estimated to be as high as 25 billion world-wide). Even now, current systems which perform post-2000 forecasting or transactions have already begun to experience failures, and such failures are likely to increase as the Year 2000 approaches due to other date-related problems in computer systems.

3. Given the interdependence of economies and the potential for cross-border disruption, the problem is not solely a national issue. In many areas, international actions have been initiated to co-ordinate remediation, testing and contingency planning, especially in collaboration with developing countries, where awareness of the issue remains low, and action is lagging. While this report focuses on OECD Member countries, it is hoped that information provided on national and international actions will encourage further international co-operation, and that it may also be of use to non-OECD countries as they

work to address the problem. The World Bank has taken the most active role in addressing non-OECD countries, including provision of grant funding for governments to plan and undertake remediation efforts, as well as organising a series of seminars to increase awareness and understanding.

Economy-wide impacts

4. Concerns have been expressed about the vulnerability of certain key sectors such as utilities, telecommunications, financial services, transportation, and government services, which have strong links to all sectors of the economy and rely heavily on massive data exchanges through large-scale information networks. There is also great concern about the status of safety-critical systems, notably with respect to health services, nuclear energy generation, defence, and air travel. A review of available data suggests that compliance levels appear to be particularly worrisome within the health care sector, some sectors of government, and small and medium-sized enterprises. Status by sector and remediation activities under way are described in Part I of this report, while Part II addresses governments' role and actions.

5. Most studies have concentrated on the direct costs of fixing the problem, mainly because it is easier to estimate this than the probability and effects of non-compliance, though still subject to a wide margin of error. Estimates of world-wide costs of addressing the Year 2000 problem range from US $300 bn by the US Fed to US $1.6 trillion by Software Productivity Research (see Annex Table 1 in Part I). The most widely quoted figure is that of the Gartner Group, which has estimated that the cost of a global fix could reach US $300-600 bn. This estimate is based on cost per line of code and excludes both consequential disruption losses and chip replacement costs. The Software Productivity Research (SPR, 1997) estimate includes (among others) US$ 530 bn for initial software repairs, US$ 454 bn for database repairs, US$ 300 bn for litigation/damages, and US$ 76 for hardware chip replacements.

6. However, the most significant effects on overall economic growth would come from service interruptions caused by non-compliance, rather than from the direct spending on fixing the problem. There is considerable debate regarding the extent of overall macroeconomic impacts, due to the great difficulty in determining how well preparations will go, and the extent to which interruptions in service, delays or breakdowns will actually occur and lead to business failures and other economic losses. Data is also not conclusive on the extent to which current Y2K spending will have related benefits in terms of upgraded IT systems that could lead to productivity gains.

7. Given the high degree of uncertainty about these underlying (and often unstated) assumptions, as well as the lack of a solid analytical framework to assess the impact of these assumptions, few analysts have attempted to forecast the macroeconomic effects of Y2K. Nevertheless, some initial studies have been conducted for *Canada, Korea, Netherlands, United Kingdom* and *United States*, as well as a number of broader studies by the financial industry, management and IT consulting firms. Among the main areas of concern highlighted in most studies are:

- short-term inflationary pressures in countries close to their peak in the economic cycle due to demand for new investment, supply-side disruptions, and significant wage increases;

- negative reactions from financial markets as the level of Y2K-related risk of firms and countries becomes more apparent;

- possible declines in productivity growth, and;

- a transitory drop in output due to a significant number of failures in critical information systems throughout the economy.

8. It appears from current data that even lower range estimates would indicate potentially significant economic impacts. Most studies to date have suggested negative economic impacts in the range of 0.3% to 1.1% of GDP over the next two years. Edward Yardeni, chief economist of Deutsche Bank Securities, has suggested a 70% chance of a serious global recession (as severe as the 1973-74 downturn during which real US GDP dropped 3.7%), based on a more pessimistic assumption of how well preparations are going.

9. In addition, the majority of studies suggest that the most likely scenario would involve negative overall effects of Y2K in the short-run, and more positive outcomes in the medium-term as Y2K offers an opportunity for firms and governments to review their IT portfolios, replace outdated systems, and enhance the future productivity of their investments. It appears that a significant share of expenditures will involve moving forward investments which in many cases would have taken place in any case at a later stage.

10. OECD countries could also suffer negative effects from non-compliance of trading partners, given their global economic interdependence. Although the quality of the data is erratic, industry experts feel that a major impact could come from disruptions in Asia where the currency and financial crisis has slowed down Y2K remediation efforts.

11. The degree of uncertainty on the pace of repairs and testing activities, and the lack of a clear picture on the global status of governments and firms makes economic forecasting of Y2K a particularly challenging exercise. Even if the probability of worst-case scenarios is relatively low, the potential for major disruptions should not be underestimated or overlooked.

Governments' Role and Actions

12. The state of government Y2K preparedness is often cited as a major economic and social concern, including the potential for loss or corruption of data, and service delays or break-downs in such areas as tax administration, customs, defence, emergency services, payroll, pension, social benefits and procurement systems, among others. Results of reviews of public sector remediation efforts in a number of OECD countries suggest that while progress is being made, there is a long way to go.

13. Governments also have a wider role to play in ensuring that the Year 2000 problem is addressed economy-wide -- by highlighting vulnerabilities and lack of preparedness; encouraging or requiring information disclosure to promote accountability and create incentives for action; or using a range of policy instruments at their disposal to facilitate or speed up preparations, such as through regulation, tax or budget incentives.

14. Responding effectively poses a major public management challenge, requiring efforts to assess and understand the extent of the problem, to develop appropriate policy responses, to establish mission-critical priorities, to raise awareness and motivate action, and to co-ordinate and implement action plans. As US President Bill Clinton recently stated, "With millions of hours needed to rewrite billions of lines of

code, and hundreds of thousands of interdependent organisations, this is clearly one of the most complex management challenges in history."[1]

15. An overall review of government responses to the OECD questionnaire suggests that most of those governments responding are well aware of the problem and have embarked on a wide range of efforts aiming to address public sector readiness and to raise awareness throughout their economies. Nearly all OECD countries have established national co-ordinating or awareness-raising bodies. Most often these are separate task forces, but several countries have established co-ordinating responsibilities within existing ministries, often divided between two ministries: one responsible for the public sector, the other for economy-wide awareness. International co-ordination is sometimes handled through these task forces, but more often through Foreign Affairs and sectoral ministries.

16. About half of OECD countries have also developed targeted priorities for preparations of the economy as a whole. Almost universally mentioned priority sectors are energy, communications, financial, transportation, health, and water supplies. Within the public sector, most frequently mentioned priorities were defense, disaster management, welfare and pension payments, and revenue and tax collection.

17. To ensure implementation, nearly all OECD countries have established government Y2K reporting systems, usually addressing public sector preparations and less frequently also including reviews of private sector preparedness. Though some OECD countries do not make their results public, results provided from 12 OECD countries' reviews indicate a mixed level of preparedness. While progress is being made, clearly the majority of work remains to be done, including much work on the time-consuming testing phase.

18. Many countries cite devolved budget management policies promoting responsibility for addressing the problem at the agency level, and suggest that agencies can address the problem from within existing budget envelopes. But a handful of countries pointed to explicit policies to set aside supplementary funding targeted to priority and problem areas (e.g. *Australia, Ireland, Japan, Korea*, and the *Netherlands).*

19. While most countries have not specifically adopted Y2K regulatory strategies, a few countries are taking interesting approaches in this area: *Denmark* has reached agreement with its accounting societies that their annual reviews of businesses will include review of Y2K preparedeness; *Denmark, Netherlands* and *Sweden* have reached voluntary agreements with IT suppliers on Y2K compliance certification schemes; *Netherlands* reviews all proposed legislation for its impact on capacities to address the Y2K problem; and the *U.S.* has proposed legislation to limit liability for private sector sharing of information on how they are dealing with the problem.

20. About half of OECD countries said they had carried out government-wide risk assessments and had at least begun contingency planning to ensure continuing operation of government services even in the event of unforeseen system or sectoral failures. Review and remediation involving embedded systems is cited as a particular risk area requiring significant attention.

1. From July 13, 1998 Clinton speech on the Year 2000 Problem given at the National Academy of Sciences.

Conclusions

21. While not every country is lagging in the areas highlighted below, there is reason for concern in many countries, and a need for sustained action in the following 10 areas:

A stronger role for governments

1) **Governments need to accelerate their own preparations.** Even governments that are often cited as world leaders in addressing the Year 2000 problem generally indicate that they have done **less than half** of the work required to achieve public sector compliance. This is particularly worrisome in light of many experts' view that systems ideally should be ready by the end of 1998, in order to avoid early manifestations of the Year 2000 problem in 1999.

2) **Governments have an important leadership role to play in promoting economy-wide preparedness.** Whether through policy actions, co-operative problem-solving with the private sector, or the more common emphasis on awareness-raising and information provision, governments can and must help to ensure that their economies are prepared for the Year 2000.

3) **Further scope exists for policy action to support Year 2000 readiness.** A number of countries have proposed or adopted proactive policy or regulatory initiatives to support private sector readiness, such as tax breaks, loan programmes for small businesses, training or other policies to encourage expansion of the IT specialist labour pool, and policies to promote information disclosure. Governments should assess such potential solutions in their own national contexts to determine the appropriateness of further policy action.

Lack of awareness is still a major problem

4) **Awareness and educational efforts are required to overcome incomplete understanding of the problem.** There continue to be misconceptions about the nature and scope of the problem in some governments and parts of their economies. National and international initiatives targeted toward vulnerable sectors or groups is a necessary part of the solution.

5) **Regular public disclosure of government and industry assessments of readiness will help motivate action.** They can also help to build public confidence that remedial action is going forward. However, governments should also be careful to balance the need for information to assess the state of preparedness, versus the additional information-collection burdens that such reporting requirements impose.

6) **Greater focus is needed on embedded systems.** The vulnernability of embedded systems or chips, built into most modern electronic equipment, is too often overlooked. Detailed inventorying, consultation with suppliers and testing is necessary to minimise problems. Contingency planning should also address the possibility that vendors' assurances about the compliance of embedded systems may be incorrect.

7) **Regional and local governments should be just as concerned.** Just as small and medium enterprises tend to lag behind larger companies in their preparations, evidence suggests that local governments often lag behind national governments in preparing for the millennium date change. While national governments may lack leverage to ensure local government

compliance, they can target regional and local government awareness and data exchange activities as part of their national campaigns.

Bringing government action to bear

8) **Y2K requires high-level managerial attention and a central strategic capacity.** The interdependence of many government information systems and the need to undertake testing involving multiple actors makes this particularly important.

9) **Risk assessment and contingency planning are an essential part of preparations.** Regardless of how well national governments prepare to ensure that their own operations are Year 2000 compliant, they will remain dependent on electricity, telephone systems, transportation and supply systems to continue functioning beyond the Year 2000, and it is virtually impossible to guarantee that all of their own systems will be "bug-proof."

Greater international co-operation is essential

10) **Increased cross-border testing and international co-operation is needed.** Transport, telecommunications, international financial transactions, energy provision and many other activities depend upon cross-border interchanges that could be vulnerable to Year 2000 breakdowns. While there is at least some awareness and institutional capacity to address the problem in most OECD countries, vulnerabilities could also arise to the extent that OECD economies interact with less prepared developing countries. While international initiatives have been launched in most sensitive sectors, greater participation will be needed to ensure their success.

INTRODUCTION

Scope of the Problem

1. The "Year 2000 problem" and the potential threat that it poses to information technology-dependent infrastructures presents a serious global economic and governmental challenge. The so-called "Millenium bug" places at risk information networks that have become pervasive throughout the OECD and much of the world. Concerns have been expressed about the vulnerability of certain key sectors such as utilities, telecommunications, financial services, transportation, and government services, which have strong links to all sectors of the economy and rely heavily on massive data exchanges through large-scale information networks. There is also great concern about the status of safety-critical systems, notably with respect to health services, nuclear energy generation, defence, and air travel.

2. On a technical level, "the Year 2000 problem," also known as "Y2K," refers to the situation whereby most computer systems currently in operation are set up to identify calendar dates only through the last two digits of the year. Programmes may fail or at least fail to function correctly as date-based calculation systems produce erroneous results. This problem stems from early programmers' need to save memory in writing software or chip design. Without conversion, many existing systems will not recognise "00" as "2000", but as "1900" (or as an invalid date). Problems may arise not only in computer systems, but also in communication networks and in chips integrated into industrial control systems, consumer electronic devices and safety systems[2]. Although the failure rate of such "embedded systems" is very low (experts estimate a 1 to 3% range), the sheer number of such hidden devices presents a significant challenge (the number of installed chips is estimated to be as high as 25 billion world-wide). Even now, current systems which perform post-2000 forecasting or transactions have already begun to experience failures, and such failures are likely to increase as the Year 2000 approaches due to other date-related problems in computer systems.[3]

3. Whereas most large companies seem to be reacting to the problem, there is concern about smaller companies where awareness is lower and funds are less readily available. Due to the high degree of uncertainty involved and the lack of precedents, many analysts, including in the insurance industry, have had difficulty assessing the true scale of the risks (Swiss Re, 1997). Painstaking conversion to computer systems ahead of the year 2000 is certainly proving costly in terms of financial and human

---

2. The Institution of Electrical Engineers (IEE) in the United Kingdom has published a comprehensive list of embedded controllers which could be vulnerable to Y2K failure, covering the following activities: manufacturing and process control, construction industry, transportation, buildings and premises, domestic services, communications, office systems and mobile equipment, banking, finance and commercial activities, medical diagnostics, monitoring and life support, testing, monitoring and diagnostic systems. http://www.iee.org/2000risk/guide/year2k20.htm

3. An example is 9 September 1999, since "9999" was a favourite code for expressing "END" among programmers in the sixties. A further complicating factor is the leap year calculation: 2000 is evenly divisible by 400 and therefore the year is a leap year, although many computer programmes and electronic devices might not recognise this.

resources[4]. Whether this will exacerbate, or create, a shortage of skilled personnel such as software engineers is a matter of keen debate, although the salaries for certain categories of IT professionals (e.g. COBOL programmers) have already seen significant raises. Developed countries are increasingly relying on qualified labour from developing countries (e.g. India), and some OECD countries such as the *United States* and *Canada* have started to review certain temporary immigration programmes in order to address potential skill shortages.

4. A number of "Year 2000" analysts cite a particular concern about the state of government preparedness. Concerns about the viability of government operations include the potential for loss or corruption of data, and service delays or break-downs in such areas as tax administration, customs, defence, emergency services, payroll, pension, social benefits and procurement systems, among others.

5. In terms of total size and spending alone, government plays an important role in the economy, through the flows of goods, services and costs between it and the private sector (general government outlays in OECD countries range from 13 to 60 percent of nominal GDP, with most in the 30 to 54 percent range). Its role in collecting, exchanging and disseminating information and its heavy reliance on information technology make its Year 2000 compliance particularly critical.

6. Governments also have a larger impact on the economy, through the laws and policies they adopt, the services they provide, and the conditions they establish to promote overall economic growth and social cohesion. In this context, they also have a wider role to play in ensuring that the Year 2000 problem is addressed economy-wide -- by highlighting vulnerabilities and lack of preparedness; encouraging or requiring information disclosure to promote accountability and create incentives for action; or using a range of policy instruments at their disposal to facilitate or speed up preparations, such as through regulation, tax or budget incentives.

7. If the problem is effectively addressed, impacts on the world economy and populations could turn out to be minimal. If not, however, impacts in any particular sector could have major and potentially critical impacts on others. An interruption in electricity generation or transmission is the most obvious case: telecommunications systems, computers and businesses cannot function without it. But others could be nearly as debilitating: if water supplies are interrupted, computer cooling systems could malfunction and cause system shutdowns. A telecommunications system breakdown would halt data exchange, including the ability to conduct electronic commerce. If transportation systems falter, manufacturing systems dependent on just-in-time supply delivery could come to a halt. If computer systems distort or destroy data, these corrupted data can have a rippling effect on other information systems as they make their way around the globe. International trade and supply chains are also dependent on the continued functioning of the weakest link in the chain in order for international commerce to continue. Given the interdependence of economies and the potential for cross-border disruption, the problem is not solely a national issue. In many areas, international initiatives are needed to co-ordinate remediation, testing and contingency planning, especially in collaboration with developing countries, where awareness of the issue remains low, and action is lagging.

4. There are various technical solutions for fixing the problem, the main ones being date expansion (increasing the year field to 4-digits), date compression (storing dates in binary or packed decimal formats), "windowing" (splitting the century into past and future windows, either fixed or sliding), "encoding" (recoding years to a new numbering scheme), and "encapsulation" (shifting the date backwards on internal clocks, usually by multiples of 28 years). (IBM, Pirkle & Associates)

Scope of OECD Report

8. All OECD countries agree on the importance of taking action to address this problem.[5] The need to complete such action is urgent, given the view of many experts that systems should actually be ready by the end of 1998 in order to avoid Year 2000-related malfunctions that are likely to occur with increasing frequency in 1999. This report is aimed at supporting such efforts by providing information on the nature and extent of the problem, on how it is being addressed, and on where there is scope for further action. **Part I** on "Economy-wide Impacts" provides an overview of the current status of Y2K preparedness in Member country economies, highlighting vulnerable sectors, noting international initiatives under way to support remediation efforts, and comparing studies on economic effects.

9. **Part II** focuses on "Governments' Role and Actions" because of the particular concerns that have been raised about their preparedness, as well as because of the important role they play in addressing the problem, both as a large user of information systems within the economy, and in promoting action economy-wide. A **concluding chapter** highlights areas of continuing concern where further action is needed.

10. While experience and policy vary as to the appropriate government role and actions required to address the Year 2000 problem, there does appear to be a core set of activities which most OECD countries are undertaking. This report does not represent an attempt to promote a single viewpoint of best practice. Differing national political systems, cultures and conditions across the OECD do not allow for identification of a universally applicable model for success. However, an examination of economy-wide impacts and country experience can help to focus on critical areas of concern, and highlight common and innovative approaches which may be referred to as governments and the private sector seek to address the problem and adapt solutions to their own circumstances. **Annex A** provides a list of World Wide Web sites in OECD countries and other international organisations to facilitate gathering of more detailed information. The OECD's own Web site will provide an ongoing and up-to-date source for linking to additional information on the Year 2000, at http://www.oecd.org/dsti/sti/it/infosoc/news/y2klinks.htm. **Annex B** provides a list of contacts in Member countries to support additional follow-up as necessary.

Methodology and Constraints

11. Research for this report involved two main approaches to information collection: **Part I** on economy-wide impacts was based primarily upon a review of existing studies and media reports. The section of Part I dealing with small and medium-sized entreprises (SMEs) also drew upon information gathered from a questionnaire about SMEs, electronic commerce and Y2K sent to Member countries.

12. **Part II** relied primarily upon government responses to an OECD questionnaire (**Annex C**) sent to all 29 Member countries at the end of May, with replies requested by late June. Information on Member country practices in this report therefore generally only reflect developments through the first half of 1998. Governments were asked at a minimum to indicate yes or no answers to 16 questions to

5. The April, 1998 Communiqué of the OECD Council at Ministerial level stated: "As the Year 2000 approaches, Ministers agreed on the importance of rapidly adapting computer systems in order to avoid the potential for significant disruption due to the so-called 'millennium bug'. They stated their intention to meet this challenge and recognised the need to exchange information among governments, and to work with the private sector, as appropriate, to ensure that the problem is revised in a timely and comprehensive manner. They also called on the OECD to promote global awareness of the Year 2000 problem and its potential economic impact, and to report to the Ottawa ministerial conference on electronic commerce."

provide some common basis of comparison, and to the extent possible to provide explanations along with their answers. A conscious decision was made to keep the questionnaire relatively brief to help ensure responses from as many countries as possible. The 16 questions address four general areas: *1)* how governments are assessing the extent of the problem; *2)* their policies and priorities for addressing it both within the public and private sectors; *3)* institutions for building awareness and co-ordinating action; and *4)* public management approaches for ensuring that policies are carried out effectively.

13. Information from the questionnaires was supplemented by telephone and written inquiries, meetings, Web site searches, and review of media reports and "Year 2000" studies addressing Member country actions and preparedness. In addition, the work of other international organisations and associations provided input into the OECD work, including, among others, reports by the European Commission, the International Council for Information Technology in Government Administration, and the Joint Year 2000 Council (a joint initiative of the Basle Committee on Banking Supervision, Committee on Payment and Settlement Systems, International Association of Insurance Supervisors and International Organisation of Securities Commissions).

14. Just as not every country has achieved the same state of readiness, not every government has the same capacities to respond to questionnaires. Though 26 of 29 countries provided at least yes or no replies to the OECD enquiry, not all were able to directly answer the questions, and some provided little or no explanation.[6] The OECD is not in a position to judge whether failure to provide information signifies a lack of preparedness and/or low priority given to addressing the problem; or rather, a lack of priority or capacity to respond to questionnaires, such as in cases where decentralised approaches make information-gathering particularly difficult. Greater facility within the OECD Secretariat to review information in English and French than in other languages and the predominant use of English on the World Wide Web also risks creating a bias in favour of countries that operate in these languages. Therefore, the absence of particular OECD countries or minimal information on their progress should not be taken as an indication that these countries are lagging behind the others in their preparations. The report provides a "snapshot" of self-reported preparations as they stood in the early summer of 1998, and identifies approaches and practices that may hold promise for others to consider. Given the consequences of a failure to prepare, governments themselves have every incentive to carry out their own assessments of their readiness, drawing upon information provided in this report or elsewhere, to facilitate planning and necessary action.

15. This report focuses on OECD Member countries, though information provided here may also be of use to non-OECD countries as they work to address the problem. The World Bank has taken the most active role in addressing non-OECD countries, including provision of grant funding for governments to plan and undertake remediation efforts, as well as organising a series of seminars to increase awareness and understanding.

6. As of 30 July, *Greece* had not responded, while *Luxembourg* and *Portugal* offered partial responses. These and a few other countries that provided minimal written explanation to supplement their answers are therefore touched upon only briefly in this report.

PART I: ECONOMY-WIDE IMPACTS OF THE YEAR 2000 PROBLEM

16. Though there is widespread agreement on the need to address the Year 2000 Problem, viewpoints are far more diverse on what its actual consequences will be. A wide range of scenarios have been put forward by analysts. Worst case scenarios suggest large-scale systems failures, delivery of government services seriously disrupted (e.g. welfare and pension payments, tax collection/refunding, postal services, access to or accuracy of official records), infrastructure gridlock (e.g. utilities, transportation networks), safety or security hazards (e.g. air traffic, nuclear plants, military systems), and financial breakdowns. A best case outcome could involve minimum disruption due to compliance of all mission-critical systems, and limited problems due mostly to incorrect results from upstream suppliers or support services.

17. Due to the high degree of uncertainty, it is impossible to forecast any precise outcomes, although it would appear that if the pace of remediation efforts continues to accelerate, the most likely scenario would be some combination of the best and worst cases, with wide variations between countries. The scope of this chapter is to examine reports on preparedness in some of the most critically important sectors, to highlight related international initiatives, and to review the range of studies that have been undertaken on the economic impacts to develop a clearer picture of what the most likely impacts may be.

18. An assessment of the impacts of the Year 2000 Problem must also take into account two current major economic developments: the Asian financial crisis, and the move towards European Economic and Monetary Union (EMU). The crisis in emerging Asia is already affecting domestic demand in many countries in that region (OECD, 1998), and Y2K might not be perceived as a high-priority issue by many firms and governments. An example of particularly vulnerable organisations are Japanese banks, which have been facing severe bad loan problems that could seriously undermine their ability to divert resources to Y2K repairs. In Europe, and in financial centres around the world, the development or conversion of software in connection with the Euro will largely be concurrent with Y2K work. One in five organisations in Europe estimates that more than 40% of their IT budgets will be spent on the Euro problem over the next three years, exacerbating the problem created by Y2K fixes (EITO, 1998). Although some scale efficiencies might exist between the two projects (such as compiling system inventories), initial evidence suggests that, especially in the case of large organisations, these projects must be run in parallel, resulting in potential competition for resources (EITO, 1998; Moody's, 1998).

19. The economic effects of the Millennium Bug can be quantified in various ways: first the direct cost to governments and firms of resources diverted to fix or replace non-compliant systems. These costs relate to error detection, fixing, and testing, with the latter often accounting for more than half of the total costs. Estimates of the world-wide cost repair range in the hundreds of billions of US$[7]. The direct fix costs will vary across industries depending on their level of reliance on IT systems and their degree of interconnectedness.

---

7. These estimates are significantly higher than those of many other major disruptions: Vietnam War US$ 500 bn; Kobe Earthquake: US$ 100 bn; Los Angeles earthquake: US$ 60 bn. The 1973-74 downturn after the Oil Crisis resulted in a 3.7% drop in real US GDP.

20. It is possible that direct spending for fixes might have positive direct and indirect short-term effects such as business for software firms; employment for IT workers, and longer-term positive outcomes due to the improved efficiency of information systems and better knowledge by firms and governments of their IT portfolios. Nevertheless, these will most probably not offset negative shocks since many expenditures are related to fixing existing capital stock instead of increasing or improving it. Given that funds to solve Y2K problems are mostly drawn from IT budgets, the main initial effect could be a slowdown in productivity growth due to resources being (temporarily) diverted from new value-added projects.

21. Another larger type of costs are the "secondary" costs due to non-compliance of systems such as billing errors, delayed payrolls and tax collection, and potentially explosive insurance and litigation bills. Some analysts have begun to speculate about how these costs translate into possible macroeconomic effects which could be observed due to wide-spread business disruptions such as negative reactions from financial markets, a significant number of firm bankruptcies, major failures in critical sectors, or inflationary pressures. The likeliness of such economy-wide effects is still a matter of debate given the complexity of the issue and the high degree of uncertainty concerning the compliance status of firms and governments both within and outside the OECD area[8].

Current status: survey evidence at the firm level

22. Although the level of awareness of the issue has been increasing throughout the world in the last year, a wide disparity between countries and among firms still exists with respect to both understanding of the issue, and progress in remediation activities. Surveys are being conducted in various countries to assess the compliance status of the public and private sectors, as well as to highlight possible sectoral impacts. Various surveys (e.g. World Bank) suggest that there is still a severe lack of awareness and action throughout many countries, and that the situation in developing countries is particularly alarming.

23. The interconnected nature of the problem raises compliance concerns at both a national and international level (the "domino effect"). The on-going process of globalisation of OECD economies and the importance of information networks throughout a wide range of economic activities increases the risk of systemic failure: even if firms within a country have achieved internal compliance, they will still be dependent on the compliance status of their (national and foreign) suppliers and customers, as well as local and national government.

Recent surveys

24. IT and management consultancy firms have been conducting periodic surveys of the Y2K issue, although some of the results of these surveys should be interpreted with care since these firms are in many cases interested parties. Nevertheless, these surveys provide useful information that can be complemented with and compared to surveys from official sources, as governments are now beginning to conduct their own studies to assess the Y2K situation at a nation-wide level, allowing for a more detailed analysis by

8. Given the degree of uncertainty and the difficulty of developing meaningful estimates, Y2K impacts are not separately estimated in OECD economic forecasts. However, to the extent they are reflected in available economic indicators, or in other factors which are considered in assessing likely future developments (such as business survey results), they are taken into account.Governor Edward W. Kelly Jr. of the United States Federal Reserve Board declared at a US Senate hearing that "it is impossible to forecast the impact of this event, and the range of possibilities runs from minimal to extremely serious." (28 April testimony).

sector, and firm characteristics. A good example of this approach is the series of reports by *Canada's* Task Force Year 2000. These reports which point to vulnerabilities and note progress across a range of sectors. Broad-ranging reports have also been developed by *New Zealand's* Government Administration Committee, the *UK's* House of Commons Science and Technology Committee, and several *U.S.* Congressional committees.

Private sources

25. During 1996, through early 1997, International Data Corp. (IDC) conducted its *1997 Global IT Survey*, one of the first world-wide surveys to examine the status of readiness of firms by size, and region (US, Western Europe, Asia), across 11 vertical industries. World-wide, by early 1997, only 7.9% of firms had completed their Y2K efforts, while 42.7% were currently working or had planned to start work on the issue, and fully 30.6% had not yet addressed the problem (see Table 1.1). The survey highlights significant regional variation: almost 45% of Asian companies had not yet addressed the problem. Firm size (based on both revenue and number of employees) appears to be a strong determining factor, with larger firms being consistently ahead, and the greatest disparity between small and large firms being found in the US. A potentially worrisome result was that more than half of small Asian firms had not yet addressed the problem.

26. Cap Gemini, the largest European computer consultancy firm, has been compiling a "Millennium Index" based on interviews with 1 100 firms, to study the size and impact of the Y2K problem in Europe and the US, as well as the level of preparedness of firms. Key findings of their study were published in April 1998 and cover 12 OECD countries[9]. Cap Gemini estimates that 1 in 7 (13.6%) organisations in Europe and the US will not complete Y2K work on time; for individual countries, this estimate ranges from 1% of firms in France to 74% in Germany, although the extent and potential seriousness of unfinished repairs in each country were not specified (and might vary widely). This wide variation between countries is mostly due to different estimates in anticipated costs which run from 90% of annual IT budgets in Germany (due to late start-up) to only 20% in France. The survey also shows that overall, only 28% of total budgets had been spent to date. The highest percentage being 30.9% in the US versus only 16.0% in Italy and 16.9% in Germany.

9. The 12 OECD countries are: Belgium, Denmark, Finland, France, Germany, Italy, the Netherlands, Norway, Spain, Sweden, the United Kingdom, and the United States.

Table 1.1. Status of Y2K readiness by region and firm size, January 1997

Percentage and total number of firms

	No changes needed	Not yet addressed	Planned/in progress	Completed	Total	
United States						
Small	15.6	46.4	31.3	6.7	100	418
Medium	17.6	25.4	48.2	8.8	100	193
Large	12.2	20.6	60.4	6.9	100	467
Total	14.5	31.4	46.9	7.1	100	1 078
Western Europe						
Small	23.0	33.7	34.9	8.4	100	3 809
Medium	20.9	20.7	48.3	10.1	100	1 115
Large	14.9	11.7	65.2	8.2	100	1 748
Total	20.5	25.8	45.1	8.6	100	6 672
Asia						
Small	17.9	53.4	25.5	3.2	100	1 057
Medium	11.2	42.8	39.5	6.5	100	430
Large	15.4	32.9	41.6	10.0	100	817
Total	15.8	44.1	33.9	6.3	100	2 304
All regions						
Small	21.4	38.6	32.8	7.2	100	5 284
Medium	18.1	26.7	46.1	9.1	100	1 738
Large	14.6	18.8	58.1	8.5	100	3 032
Total	18.8	30.6	42.7	7.9	100	10 054

Note: Firm size is based on annual revenue: small firms are those with revenues under US$10 million, medium for those with revenues between US$10-50 million, and large firms are those with revenues exceeding US$ 50 million.

Source: IDC *1997 Global IT Survey* from IDC (1997).

27. An IBM survey from early 1997 of 1 781 corporate customers gives another picture of the overall status by industry. The survey reveals that more than 40% were implementing changes, and between one-fourth and one-third were conducting assessments. The finance, distribution, manufacturing and health sectors were well ahead in their projects (more than 60% reported having completed or on being on the verge of completing projects). The lowest level of readiness was found in the utilities, government and transportation sectors. This study also provides some information on the approaches that firms are using to solve their Y2K problems, indicating that most firms are conducting in-house repairs with no external help, or purchasing standard fix packages.

28. Another IT consultancy firm, the Gartner Group, uses a 5-level scale ("Compare Scale") to measure levels of Y2K compliance[10], then assesses the status of firms by industry and country (15 000 firms across 23 vertical industries in 87 countries) based on the number of respondents at each level. Table 1.2 summarises Gartner's recent analysis.

10. The 5 levels are: 1 - Preliminary activity, 2 - Problem determination, 3 - Plan complete and resources committed, 4 - Operational sustainability, and 5 - Fully compliant.

Table 1.2. Y2K readiness status by country

Status	Countries / regions
Ahead	United States, Australia, Canada
3 months behind	Holland, Belgium, Sweden
6 months behind	United Kingdom, South Africa, Israel, Ireland
6-8 months behind	Japan, Switzerland, Italy
8-12 months behind	Germany, rest of Middle East
12-14 months behind	Argentina, Mexico, Russia, Taiwan, Malaysia
18-24 months behind	China, Thailand, the Philippines, Central Africa

Source: Gartner Group (1998).

29. The Japan Information Service Industry Association (JISA) conducted a survey in July 1997 to study the status of Japanese firms (JISA, 1997). The approximately 1 300 responses indicate that although awareness has been increasing, some concerns remain with respect to smaller and/or rural businesses (see section on SMEs). Less than 16% of responding firms had completed their projects, while only 24.3% of those not having completed their projects planned to do so by the end of 1998, and 23.9% by early 1999, and many firms are already foreseeing delays due to testing activities.

30. Coopers & Lybrand published in November 1997 a survey of Y2K status of large firms in Australia (C&L, 1997). A result indicative of the need to urgently address the issue, was that almost one-third of respondents had already experienced Y2K problems in their business activities (see Box 1). It appears from the survey that the Government sector has the highest risk of late project completion. Projected Y2K costs averaged 14% of annual IT budgets, with the highest ratios in the manufacturing sector (73%) and in investment management (41%).

Box 1. **Examples of early Y2K-related problems**

The Coopers & Lybrand survey of Australian firms reveals 31% of responding firms had already experienced Y2K-related disruptions to their business before the end of 1997. Here are some examples of problems, from various sectors:

- banks could not issue credit cards with expiration dates past 2000. In many cases a '99' expiration date had to be used; similar problems were reported by medical companies with expiration dates on their products;
- purchase orders could not be input into a software package purchased as "compliant";
- inability to process leases, securities, orders and other transactions extending beyond 2000;
- travel companies had experienced problems with advanced bookings more than 2 years ahead;
- automatic inventory ordering systems had halted in some cases;
- a health insurance company reported problems with claims payments systems which provide for reduced rates of compensation at two years after the injury date.

Source: Coopers & Lybrand (1997).

Government surveys

31. In Canada, Task Force Year 2000 published a first report "A Call for Action" (Canada Task Force 2000, 1998*a*) highlighting the importance of the issue. The study published in February 1998 was complemented with a survey by Statistics Canada, the results of which are included in another report (Stats Canada, 1998*a*). This survey of 2000 Canadian businesses reveals that by the Fall of 1997, about half of them had taken specific actions to address Y2K, including those in key sectors such as transportation, communication and utilities. The figure was even lower for the primary sector where only about one-third of firms had taken formal action. A follow-up survey conducted in May 1998 reveals that firms are stepping up remediation efforts, with small firms tackling the problem in a more systematic manner: 66% had taken action, as compared to 39% in the previous period (Canada Task Force 2000, 1998*b*; Stats Canada, 1998*b*). The share of firms that are taking steps to verify the compliance of their suppliers, customers and service providers remains low, but has more than doubled from October 1997 (from 13 to 28%). The greatest concern for Canadian authorities relates to delays in action by firms in the utilities sector and small firms throughout the economy.

32. The New Zealand Government Administration Committee released a report in April 1998 on budgeted costs and public sector status (New Zealand GAC, 1998). Among the main findings were that fixing costs could exceed NZ$ 120 million for the public sector and NZ$ 450 million for the private sector. The main concern was small and medium-sized businesses (50% of firms with less than 250 employees had not yet addressed the issue), since it was estimated that a month-long disruption to the New Zealand economy as a result of Y2K-related damage to SMEs could cost the New Zealand economy up to NZ$ 2.5 bn.

33. In the United States, the General Accounting Office (GAO) has been issuing regular reports ("scorecards") on the status of public sector agencies. Testimonies from Senate and House hearings are also a valuable source of information from both government officials, industry experts, and witnesses from all areas of business. Some countries have encouraged or required public disclosure of Y2K compliance status for public firms, such as Australia, New Zealand and the United States (see Part II, pars. 138-139 regarding policy actions in this area).

34. An analysis of recent Securities and Exchange Commission (SEC) filings by the 250 largest US public firms was conducted by Triaxys Research LLC. Of the companies who disclosed Year 2000 information, two-thirds had not started work on the problem until the last two years, while one-third did not begin until 1997. Extrapolating from the data from the firms reporting projected costs, it was estimated that the top 250 US companies will spend approximately US$ 37 bn, 79 per cent of which will be spent during 1998-99. A similar analysis of the 500 largest US corporations (S&P 500 by Edward Yardeni of Deutsche Bank Securities, and Fortune 500 by the Federal Reserve Board) suggests that the total cost for the whole US private sector could reach US$ 50 bn.

Status by sectors

35. Sectors can be broadly classified according to their level of risk or exposure to the Year 2000 problem. Although difficult to quantify at an aggregate level, exposure for firms within a sector will be based on the level and type of use of information systems, their reliance on embedded chips, and the degree of interconnectedness of the industry. This measure of exposure (which is not limited to safety risks) should be broadly similar across OECD economies. Table 1.3 combines this with a measure of readiness of the given industry as a whole (based on status reports from public and private sources), which might vary widely between different countries. The table -- which is intended to give a general qualitative

assessment of exposure and compliance status throughout a broad range of countries, and not a precise measurement based on hard data - reveals that overall, although remediation activities are well under way in many industries, certain key sectors are still lagging behind.

Table 1.3. Y2K exposure and compliance by sector

	Compliance		
Exposure	High	Medium	Medium-Low
High	Finance, banking, insurance, air transport	Telecommunications, manufacturing, most government services, energy	Other government services, health care, retail trade
Medium		Shipping	SMEs
Low			Agriculture, construction

Source: OECD.

36. The following section examines several sectors which are particularly vulnerable due to the importance of networks, their reliance on IT infrastructures, and their level of interaction with other parts of the economy: energy, telecommunications, financial services, transportation, health care, and small and medium-sized enterprises (SMEs).

Energy

37. Power generation and water supply are arguably the most critical areas of concern, since major disruptions in either would have serious economy-wide impacts. Energy security and supply could be compromised due to the pervasiveness of embedded systems throughout all stages of energy generation, transmission and distribution. Nuclear power plants were quickly identified as a main area of concern due to potential safety hazards in case of a failure. Dedicated transmission networks are another broad area of concern as electricity, gas, and oil supply could be seriously disrupted.[11]

38. In addition to safety hazards, failures in nuclear power plants could result in electricity supply disruptions. In many OECD countries nuclear energy accounts for a significant share of total electricity generated domestically (see Table 1.4). According to the US Nuclear Regulatory Commission (NRC), the five main areas of potential failure in nuclear power plants are: "(1) software to schedule maintenance and technical specification surveillance, (2) programmable logic controllers and other commercial off-the-shelf software and hardware, (3) digital process control systems, such as feedwater control or valve control, (4) digital systems for collecting operating data, and (5) digital systems to monitor post-accident plant conditions" (NRC Congressional testimony, 12 June 1998). The NRC has collaborated with the Nuclear Energy Institute (NEI) to develop industry-wide guidance for Y2K issues at nuclear power reactors. The NRC is requiring that all operating nuclear power licensees submit written descriptions of their Y2K plans, and has scheduled on-site random inspections to assess the status of nuclear facilities.

11. Oil production and distribution are other less visible areas of concern: metering devices and valves in pipelines could potentially malfunction, embedded chips in oil refineries could be affected, offshore oil platforms could experience failures due to their high level of automation. Nevertheless, it would appear that most major oil companies are well aware of these issues and are taking actions to address them.

Finally, the NRC is working together and sharing information with other agencies such as the Federal Energy Regulatory Commission and the Department of Energy to ensure that the reliability of the electrical grid is not compromised.

Table 1.4. Nuclear energy generation, 1997[1]

Percentage

Country	Share of nuclear in total domestic electricity generation
France	78.5
Belgium	60.1
Sweden	47.2
Switzerland	40.8
Hungary	39.5
Korea	31.2
Japan	31.1
Germany	31.0
Finland	30.4
Spain	30.1
United Kingdom	28.9
Czech Republic	19.3
United States	18.0
Canada	14.7
OECD Total	23.3

1. Estimated.
Source: IEA, July 1998.

39. In *Canada*, the Atomic Energy Control Board has testified publicly that it is conducting similar initiatives (April 21 testimony) and that it is co-ordinating certain activities at an international level with foreign agencies such as the US NRC, the *French Conseil Supérieur de la Sûreté et de l'Information Nucléaires* (CSSIN) and the *United Kingdom* Atomic Energy Authority (UKAEA). Large utilities such as Ottawa Hydro and Ontario Hydro Nuclear reported in April 1998 having completed between 40 and 50% of their programmes. The Canadian Association of Petroleum Producers (CAPP) and the Canadian Gas Association (CGA) have set up committees to assess the extent of the risk to the industries through surveys of their members and to co-ordinate remediation activities involving stakeholders throughout the supply chain. The major focus is on ensuring business continuity and developing operational contingency plans that incorporate the possibility of multiple, simultaneous and extended disruptions. Modular testing of individual components such as pipelines, compression stations and storage facilities, is already underway.

40. In addition, the Nuclear Energy Agency (NEA) has set up a network of "national co-ordinators" to exchange information on identified problems and good practices via an electronic mailbox. The NEA with the support of the Canadian authorities is organising a major workshop on the subject in Ottawa in February 1999. The workshop will review how the issue is being managed by the nuclear community.

41. The North American Electric Reliability Council (NERC) is coordinating activities between *American*, *Canadian* and *Mexican* utilities in order to ensure that the issue of interconnectedness in electricity supply and delivery systems is adequately addressed. An industry group, the Electric Power Research Institute (EPRI) has launched a programme that regroups 74 companies (accounting for more

than 70% of the US electrical power generation capacity), to co-ordinate activities and exchange information on embedded systems. A Web site has been set up, centralising information about equipment inventories, programme plans, document templates, and utility test data (http://www.epriweb.com).

42. EURELECTRIC/UNIPEDE, a network of IT experts in the energy generation and distribution industry, reported at an EC Workshop in March 1998 (EC, 1998) that the Year 2000 was their highest priority and that they would capitalise on the work already conducted in the Netherlands through a national research body, EnergieNed. The main concern appears to be a potential shortage of skilled IT professionals, from mid-1998 onwards.

Telecommunications

43. Telecommunication is a very vulnerable sector due to the highly computerised nature of networks, from switching and transmission, to billing and ordering. It is mostly the infrastructure that is at risk: a broad potential for failures exists in many network elements such as undersea cables, sea-based repeaters, satellite ground equipment, and Internet traffic (data routing)[12]. The widespread disruption caused by incidents such as AT&T's frame-relay network outage, and the recent failure of PanAmSat's Galaxy IV satellite (which disabled 90 per cent of pagers in the US) highlights the increasing dependency on telecommunication infrastructure and networks.

44. In recent testimony before the US House of Representatives, the Federal Communications Commission (FCC) confirmed that major US telecommunication carriers are well advanced in their remediation plans, but warned that smaller companies might be lagging behind. A survey conducted in early 1997 by British Telecommunications (BT) suggests that telecommunication companies in other regions might be less advanced in their programmes: only 11% of BT's commercial partners in Africa had set millennium projects, 23% in the Asia-Pacific region, 43% of European operators, and 49% in the Americas (ITU, 1998). A survey of telecommunications carriers in 113 countries conducted by the US State Department through March 1998, reveals that less than half are expected to be fully compliant before December 1999 (see Table 1.5).

Table 1.5. Y2K status of international telecom carriers, March 1998

Number and percentage

Region	Compliance expected by the end of 1998	Compliance expected by the end of 1999	Addressing Year 2000, but having problems	Unaware or not begun	Total
Central and South America	4	2	4	5	15
Europe and Canada	8	15	9	9	41
Africa	2	1	10	9	22
East Asia and the Pacific	8	6	5	4	23
Near East and South Asia	3	2	5	2	12
Total	25	26	33	29	113
Percentage	22	23	29	26	100

Source: US State Department, *Global Telecommunications Survey*, in Yardeni (1998).

12. The Internet Engineering Task Force (IETF) publishes a working document (Internet Draft) which contains an inventory and the Y2K status of important Internet protocols (http://www.ietf.org/internet-drafts/draft-ietf-2000-issue-03.txt).

45. Some large carriers such as AT&T (which has some 500 million lines of code to review) have announced contingency plans including network capacity expansion and time zone "quiet periods" (during which some systems are deactivated during the 24-hour transition phase). Given the complex nature and interdependency of the networks and communication systems, it is virtually impossible to recreate "off-line" Public Switched Telephone Networks (PSTN) for thorough and reliable testing. In the US, 7 large telecommunications companies have estimated their combined remediation costs to exceed US$ 2 billion (SEC filings).

46. The International Telecommunication Union (ITU) is coordinating cross-border activities and has set up a Task Force to co-ordinate awareness activities, and work on specific issues such as inter-carrier testing, and collaboration with equipment and software providers (ITU, 1998). The large European carriers are also involved in cross-border testing initiatives through the European Telecommunications Informatics Services (ETIS).

Financial services

47. This sector has been given priority attention due to its reliance on information technology, to the highly date-sensitive nature of the data that it processes, and to its globally interconnected nature. Concerns have been expressed that widespread failure in a number of sensitive areas (dealing, payment and settlement systems), could spread throughout the system and have serious global economic effects. Although banks and other financial institutions were among the first to address the issue, there exists some concern that smaller banks and credit unions could still be particularly vulnerable.

48. At an international level, the Bank for International Settlements (BIS) and the G10 Basel Committee on Banking Supervision began to co-ordinate activities encouraging banks to take prompt action and develop contingency plans due to the high systemic risk. This led in April 1998 to the creation of the Joint Year 2000 Council whose main mission is to "maintain a high level of attention on the Year 2000 computer challenge with the global financial supervisory community, to share information on regulatory and supervisory strategies and approaches, to discuss possible contingency measures, and to serve as a point of contact with national and international private-sector initiatives" (Joint Year 2000 Council, 1998). The Joint Year 2000 Council plans to set up a Web site containing information about individual countries' progress in overseeing their financial systems' Y2K preparations, thus providing a useful incentive for increased information transparency and exchange. A recent survey covering 40 industrialised and emerging market economies revealed that although many bank supervisors only initiated their assessment in late 1997, they are now well advanced in their remediation plans.

49. An industry group, the Global 2000 Co-ordinating Group, was formed in April 1998 to address the potential impact of Y2K on global financial markets. It includes a wide range of actors from the global financial community who are collaborating in monitoring three broad areas: market infrastructure, financial industry, and third-party service provider readiness.

50. At a national level, the US Federal Reserve has been active in assessing the status of banks under its supervision. The US Securities Industry Association (SIA) organised preliminary tests during July 1998 involving 29 securities firms, major stock markets and clearing and settlement firms, while full industry-wide testing is scheduled to take place during March and April 1999 with more than 1 500 participants. Results from these tests might give a first insight into potential problems at an international level. The Federal Deposit Insurance Corporation (FDIC) has mandated all federally-charted banks to give detailed plans of their remediation projects and schedules for completion. In late 1997, the first formal regulatory action was taken against a holding company and three of its subsidiary banks for

insufficient progress. The FDIC has also conducted an on-site review of 6 034 financial institutions in the United States, with satisfactory results: less than 1% of all institutions were rated as making "unsatisfactory" progress in their Y2K projects (FDIC, 1998), The Office of the Comptroller of the Currency (OCC) conducted a similar review of more than 2 500 US banks which confirms that the banking sector is ahead of most other sectors in its remediation efforts: 87% of the banks surveyed received a "satisfactory" rating on their Y2K-progress, while only 13% received a rating of "needs to improve" (BNA, 1998).

51. Large banks and financial institutions are already foreseeing costly fixes: Citicorp expects to spend around US$ 650 million, while Bank of America and Chase Manhattan have each budgeted in excess of US$ 300 million. A broad estimate by the SIA for the whole US financial services industry puts the tab at US$ 5-6 bn. Although these figures are high, a survey of the 30 largest US banks (PaineWebber, 1998) shows that total Y2K budgets range between 0.1 and 3.0% of the banks' 1998 expense base, with an average of less than 1.5%. An area of potential risk is the high dependence of banks on external vendors for many of their applications, given that the delivery dates from vendors are often later than deadlines for internally-developed systems repairs, thus pushing back testing dates; Chase Manhattan has about 2 700 applications and relies on vendors for about 90% of its software.

52. Estimates from other OECD countries also suggest a very high cost: the Reserve Bank of Australia recently estimated that the total cost for the Australian banking sector could reach AU$ 1 bn (US$ 664 million) (RBA, 1998). Japan has recently conducted a survey of its banking industry which revealed that although larger banks seem to be well ahead, smaller financial institutions appear to be lagging behind. While some observers have noted that projected spending figures for Japanese banks seem lower than those for banks in other countries (US$ 249 million for the 49 major Japanese banks), the Ministry of Finance expresses confidence that compliance will be achieved on time. The Federation of Bankers Associations of Japan has established a Y2K Roundtable for Payment Systems which will co-ordinate testing activities during 1999. The Japanese Securities Dealers Association (JSDA) has also planned to conduct extensive point-to-point (bilateral) and street-wide (industry-wide) testing during 1999.

53. Some analysts have suggested that Y2K and the Euro conversion could further the on-going process of banking consolidation in Europe as some Y2K-deficient banks become potential acquisition targets of larger financial institutions. Likewise, smaller local banks (such as German or Spanish savings institutions, or Swiss cantonal banks) might consider pooling resources to cover costly fixes through mergers (Moody's, 1998). The insurance industry is also highly concerned about the possible explosion of claims in all non-life insurance categories. The very insurability of Y2K risks is a considerable problem for insurers, since such risks do not come under the normal insurance definitions of frequency and average cost of claims.

Transportation

54. The main concern is *air transportation* due to the seriousness of safety issues, as well as the potential impact on other related industries such as tourism. Although the primary concern is with air traffic control systems, potential date problems could also arise in other systems such as reservation systems, maintenance systems, on-board navigation and flight control software. The International Air Transport Association (IATA) estimates that the world's airlines will be spending around US$ 1.6 bn to

fight the millennium bug[13]. This estimate does not include repairs to air traffic control systems, airports, computer reservations systems and other third-party vendors, nor does it include the US$ 20 million spent by IATA itself on assistance and monitoring activities among industry suppliers. In March 1997, IATA presented the results from a survey of 44 airlines which revealed that at the time, only half estimated being "50 percent or more" compliant (http://www.iata.org/y2k/survey.htm). IATA is also working closely with other associations such as the US Air Transportation Association (ATA), the International Civil Aviation Organisation (ICAO) and the Airports Council International (ACI), as well as with other international and regional bodies (*Airlines International*, May/June 98). Following concerns from many large carriers, IATA plans to publish by mid 1999 a "cartography of Year 2000" which would highlight potentially hazardous flying zones and airports.

55. The Air Transport Association of Canada (ATAC) has been collaborating with the ATA and IATA to develop a database which would cover the status of providers of air navigation services, and of airport services. With respect to air navigation systems, NAV CANADA conducted a review of its 42 mission-critical systems (those with a significant impact on information provided to controllers and flight service specialists), and concluded that 18 of those needed to be fixed. Information is being exchanged with similar agencies such as the US Federal Aviation Administration (FAA) and the Civil Aviation Authority (CAA) in the United Kingdom. NAV CANADA expects to complete all its repairs and conduct full system tests by April 1999. In the US, the FAA reported in April 1998 that 30% of its mission-critical systems were certified Y2K compliant and fully operational. For air traffic control systems, the percentage of systems repaired was higher, reaching 57% (http://www.faay2k.com).

56. Another area of wide concern is *maritime transport*, since significant delays or other disruptions in shipping activities could have serious adverse effects on global international trade. It is currently estimated that the millennium bug could affect nearly 3,000 commercial ship-owners (Ship2000). Safety-critical applications such as those dealing with navigation, communications, strength and stability calculations, engine monitoring and control, and fire detection could be subject to failure (Lloyd's Register, 1998). In early 1997, the International Maritime Safety Agency notified all governments world-wide that the 'Millennium Time Bomb' represented a significant threat to maritime shipping. However, the problem of embedded processors has only recently been properly identified by responsible bodies such as the UK Institute of Electrical Engineers and the US and UK Marine Safety Agencies.

57. Evidence presented publicly at the end of 1997 and early 1998 by Shell International Trading and Shipping Company with respect to its tanker fleet, showed that its largest and most automated ships did indeed contain dozens of embedded processors. The original equipment suppliers had reported that less than 10 per cent of these were likely to be non-compliant. However, when Shell engaged the services of a third-party to check if this information was correct, tests of the embedded processors revealed that over 20 per cent of the shipboard systems were non-compliant, and that approximately 10 per cent more were suspect for date-related failures or malfunctions. Shell has since then stated that about 80 per cent of the costs it is incurring for Year 2000 problem identification and remediation are in the area of embedded processors found in its various marine installations, ships and processing facilities (Ship2000).

58. The tests performed by the Shell's contractors found embedded chip compliance problems in the following monitoring and control systems: navigational systems and equipment, telecommunications systems and equipment, and real-time process controls (engine room and cargo monitoring and control

13. Boeing, the world's largest supplier of commercial jet aircraft, has announced that all of their major jets are in the process of being repaired in order to be Y2K compliant (http://www.boeing.com/commercial/aeromagazine/sy/sy01/index.html).

systems). Other systems where real failures of embedded processors in ships have already been observed include radar mapping, ballast monitoring, cargo loading, ship performance monitoring, engine room vibration monitoring, service aid for ships control system, and ship main control systems [14].

59. Disruptions to railway networks could result in serious damage to nation-wide transportation and distribution logistics systems. In Canada, Canadian National Railway (CN) is conducting an examination of all its safety-critical systems including signalling systems, wayside inspection and monitoring systems, crossing and other warning devices, and has established an in-house simulation network to test the reliability of its nation-wide communications network. (House testimony, 21 April 1998).

Health care

60. The health sector is highly vulnerable to Y2K damage for a number of reasons. The health care sector relies heavily on dates and time intervals - for care plans, dosages, laboratory results, expiration dates, reminder notices as well as familiar organisational and administrative requirements. It is heavily dependent on embedded systems in a variety of medical devices such as infusion pumps, diagnostic equipment, dialysis machines, defibrillators, or pacemakers. In many cases, potential failures could arise from self-checking devices which need constant and precise recalibration. It appears that although most medical equipment is not likely to malfunction[15], some medical devices have already reportedly demonstrated that they will shut down or function incorrectly.

61. As with all embedded systems, it is not clear which devices will operate normally, which ones will clearly fail (with accompanying contingency requirements) and which ones will appear to operate normally but give erroneous results; in the healthcare context the last can be a dangerous outcome. This also needs to be seen in the context of age of the equipment involved (over three years old and especially older equipment), its provenance (major manufacturers, cloned devices, etc.), especially in the context of major health funding restrictions in many countries since the 1980s, and fragmented purchasing practices by health authorities and hospitals. Most devices are mass produced and hence the manufacturers are best placed to evaluate the ability of a device to roll over at 2000. However manufacturers usually provide support for electromedical devices for a finite period only. Consequently there are many devices in use that will require in-house evaluation. Many devices may in fact be custom made in-house.

---

14. Because of its reliance on electronic navigation systems, another concern for the transportation industry as a whole is the so-called “end of week” (EOW) roll-over of Global Positioning Systems (GPS) which may suffer from a similar but unrelated problem caused by the roll-over of a counter which tracks the number of weeks from a base date. The critical date for the GPS system is midnight 21-22 August 1999, 132 days before the turn of the millennium. In addition, although all satellites are reported to be Y2K-compliant, some satellite support systems may not be, potentially affecting GPS receivers and GPS receiver-based systems by the Year 2000 rollover if they are not Y2K compliant. GPS is also extensively used in surveying and positioning activities in other sectors of the economy such as the petroleum industry.

15. A press release by the world’s largest manufacturer of pacemakers and related devices states that: “the dates beyond 12/31/99 will have no effect on the delivery of safe, effective therapy by any [of its] implantable device[s]. This includes pacemakers, defibrillators, drug infusion systems, neurostimulators, and heart valves. No therapy delivered by [such] implantable device[s] does so on the basis of any calendar date. Most time-sensitive [...] devices deliver therapy based on an internal counter. Others deliver therapy only when they sense the need. Some deliver therapy continuously or when activated by a patient-controlled activator.” (http://www.medtronic.com/corporate/yr2000/yr2000.html)

62. In addition to the possible disruption of complex medical instruments, there also exists a risk of disruption of pharmaceutical production and distribution (e.g. prescription drugs), errors in hospital administration systems (patient records, medical risk management, billing and financial applications) and laboratories as well as the possibilities of legal actions due to improper or inadequate due diligence. Despite the seriousness of exposure, a recent survey of US hospitals (Gordon & Glickson) found that 30 per cent had not yet begun year 2000 projects. The Rx2000 Solutions Institute in the US surveyed health professionals on Y2K readiness. 94% agreed with the proposition that "Y2K issues have significant potential to create errors that lead to unnecessary deaths in health care", 69% agreed to the proposition that "The healthcare industry lags behind most other industries in addressing Y2K issues" and 62% had already experienced Y2K problems (http://www.rx2000.org/sig). A study by the GartnerGroup found that 87% of all healthcare organisations were in danger of systems failures within the next two years.

63. Although there are few published estimates, some experts estimate that on average the cost to replace non-compliant medical equipment in a 400-bed hospital in the United States could reach US$15 mil. (HR&B, Vol.2, No. 2). Compliance at the level of individual hospitals and health systems could range from 30-35% of information service operating budgets over two years. In addition to cost issues, the sector is highly fragmented and interdependent, with large organisational components (insurance companies, healthcare delivery organisations, public sector funding organisations, managed care organisations, pharmaceutical companies, etc.) and huge numbers of smaller health care providers, laboratories, device suppliers, ambulances, supplies organisations, all operating within highly regulated contexts. There is no obvious major market player to drive Y2K compliance.

64. The US Food and Drug Administration (FDA) has set up a database to "provide information regarding the status or impact on product performance of the "Year 2000 Date Problem" for medical devices and scientific laboratory equipment (biomedical equipment)" (http://www.fda.gov/cdrh/yr2000/y2kintro.html). Information is provided by equipment manufacturers to the FDA through a questionnaire and made available to the public via the World Wide Web. Health Canada has launched a similar information-gathering initiative, as has the Therapeutic Goods Administration in Australia.

SMEs

65. Most developed countries are now rapidly moving to identify and deal with threats posed to SMEs by Y2K. This is amid growing concerns about SME preparedness and is understandable given their massive contribution to employment and income and the extent to which SMEs are perceived as a barometer of economic well being. Detailed assessments are lacking but fears about potential impact are considerable, albeit imprecise, in terms of the impact on SMEs themselves and flow on effects for other sectors.

66. In a number of countries, governments and large professional associations such as those in the IT industry and in banking, have commissioned and undertaken formal assessments to determine Y2K readiness by SMEs (see Box 3). Early findings indicate not only major lack of preparedness for Y2K by SMEs in general but also suprisingly high levels of non-awareness of the nature and potential impact of the problem among SMEs for their growth and indeed viability, with almost zero awareness in Eastern Europe. Optimism about preparedness in the key sectors of the economy among the developed nations is thus somewhat tempered by a very evident lag in SME preparedness and strong concerns about their capacity to be compliant and the effects of that non-compliance for them, and more broadly for the economy. For countries with a significant grouping of export-oriented SMEs, there may be concerns about trade impacts.

67. Major issues emerging are a lack of awareness by SMEs of the issue (and/or confusion due to media information overload), a lack of awareness of the need for them to do anything in the short- to medium-term, and confusion as to what should be done, how it should be done and the associated costs to the companies. This lack of awareness appears to be most marked among the smaller SMEs, SMEs in regions and in more traditional sectors of the economy.

Box 2. **Some examples of SMEs and Y2K**

A survey in Australia by the Australian Bankers Association in March 1998 found that while most SMEs had heard of the problem, there were major misconceptions about the nature and potential impact of the problem. While 80% of the surveyed companies had at least one type of technology that could be affected by the millennium bug and 60% had systems and software instrumental to running the business, over 40% did not plan to take any action and only 25% had taken action, most of it insufficient. Most overlooked the importance of supply chain dependencies.

A survey by the Japan Information Service Industry Association (JISA) examined the private and public sector approaches to Y2K in 1996 and 1997 and expressed anxiety about significantly lower awareness and lack of action among smaller and rural businesses.

A government survey in Korea in March 1998 found some 34% of SMEs planned to do nothing about Y2K.

A survey in Europe by IBM on progress toward Y2K readiness in January 1997 and April 1998 highlighted small companies (defined as 100-1000 employees), noting almost 41% undertaking no significant activity in 1997 but decreasing to only 13% in April 1998. There was some variation across SMEs by countries in terms of whether the Y2K problem was perceived to be purely technical or a more general one requiring an organisation-wide fix. Overall some 43% of responding small firms saw the problem as a technical one, significantly more so in France and Switzerland.

68. Obviously, any business or organisation with data reliant systems is at risk. SMEs are vulnerable in three ways. Firstly with regard to their own systems in-house, some surveys indicate that companies are most vulnerable the more reliant they are on computerised systems - by virtue of being in sectors such as tourism, business services and to the extent that they are export-oriented -- or simply due to importance of their accounting systems being fully computerised and that many processes essential to the business are linked -- order and supply; billing and payment; manufacture and distribution; labelling and bar coding.

69. The second area of vulnerability lies with their exposure to outside organisations or companies critically related to the SMEs operations and business, the extent to which companies may be linked by systems such as data exchange for orders, delivery, billing and banking and the extent to which these entities may not have dealt with their internal Y2K problems. Such failures in key suppliers and customers, financial institutions and utilities and the companies providing data exchange systems would have major effects on SME operations.

70. A third area of vulnerability lies with the failure of machinery and equipment that operates on time dependent embedded microprocessors. This could affect some production capacity for small manufacturers as well as essential infrastructure such as telephones, elevators, refrigerators, security systems.

71. Another indicator of vulnerability and Y2K risk is the extent to which SMEs are IT-reliant according to functions. For example, a survey conducted by the Small Business Administration (SBA) found that US SMEs are 90% reliant for accounting/finance and billing functions, 86% reliant for word processing, 80% reliant for sales recording, 75% for communicating with customers, and 60-70% reliant for database and project management, payroll, marketing and sales management and inventory/tracking

and warehousing functions. The least IT reliance was for manufacturing at 30%. In other words, to the extent that this application reliance is true, then all these essential functions are potentially affected in major ways. The age of IT systems which are used, including whether they were developed in-house and are customised, would also need to be factored in. Probably the majority of SMEs have equipment more than three years old and dated applications. Unsuprisingly, companies specialising in accountancy and finance packages are reporting massive increases in business as they upgrade existing systems and sell new ones, write code for custom modules and re-engineer.

72. Some commentators have argued that small size gives SMEs some advantages in dealing with Y2K; positive factors could be greater flexibility among some SMEs and a capacity to use readily accessible off-the-shelf solutions or to re-equip their systems. It could be argued that some of the smallest SMEs have an in-built contingency plan, to simply go off-line again. Some responses to the OECD survey questionnaire on SMEs and Electronic Commerce suggest that the introduction of electronic commerce in SMEs can simultaneously produce a "millennium-proof situation in the business systems of these companies as a result of the replacement of relatively simple software".

73. On the other hand however, some SMEs' particular vulnerability may be precisely their lack of flexibility, for example those companies that are small, family-controlled and reliant on comparatively old information technology (characteristics highlighted in recent German Chambers of Industry and Commerce reports). The willingness to incur the costs to overhaul IT equipment may be low or the cost may simply be too high, especially when the original systems were developed in-house, were customised, or even were specific to the industry. In any case, original codes may be lost.

74. SME vulnerability is particularly marked in terms of the high costs and shortage of human resources to deal with the problem (especially of the key diagnostic and IT human skills). Such shortages (and lack of expertise) can be apparent within companies and can be accompanied by a marked reluctance in some SMEs to bring in outside help. SMEs are also vulnerable in terms of access to external consulting and service assistance: surveys indicate that SMEs are only just beginning to look at the problem now and shortages of consulting and service assistance (and therefore the cost) can be expected to increase as 2000 approaches. There are indications also that SMEs that are integrated into already highly informatised supply chains as producers, suppliers and subcontractors will be very vulnerable.

75. Overall effects across the SMEs as a whole are hard to ascertain. Surveys and the literature indicate that SME compliance will vary by country, by industry sector, by market focus, by domestic or overseas market orientation, by size and age, by structure, by use of IT, by the degree of reliance on IT by function, and by type and frequency of IT purchase, to name several factors. The above-mentioned Australian study suggested a company failure rate of 10-20% was conceivable.

76. The current OECD Survey on SMEs and Electronic Commerce has a section specifically addressing Y2K issues for SMEs and a clearer picture for some of these issues should emerge from that process as well as best approaches to deal with the issue. At this stage, promising efforts targeted at SMEs involve campaigns to raise awareness (advertisements, supplements, dedicated web sites providing information, advice with some moving to develop interactive tutorials), technical support, tax write-offs, training, facilitated access to consultants and products and other forms of assistance to achieve compliance. This is usually done as a co-operative effort involving some or all industry associations, government departments, SME departments and ministries and large IT, banking and insurance companies.

Government sector

77. As mentioned in this report's introduction, governments are seen as a critical sector in part because of concerns about their overall level of preparedness, and also because of the important role they play in the economy and in ensuring the continued functioning of critical infrastructures. Many governments have encountered difficulty in estimating their own costs for undertaking Y2K fixes. In response to the OECD written enquiry on government Year 2000 preparations, many governments did not provide estimates of annual costs, but rather, total costs of addressing the problem over two or more years. Others provided no estimates at all, citing decentralised budget processes and policies that make it difficult to consolidate such information and that generally require agencies to address the problem within their existing budget. As no internationally comparable estimates have been developed on government information technology budgets (because different governments measure this in different ways, if at all), it is even more difficult to develop meaningful comparisons across countries regarding their expenditures on the Year 2000 problem. The sample of government budget estimates for addressing Year 2000 compliance provided in Table 1.6, while not strictly comparable, at least provides an indication of the magnitude of the task.

78. The issue of how governments are responding to this challenge is addressed in much greater detail in Part II of this report, including a section on how they are managing Y2K budgets.

Table 1.6. Government Estimated Budget Costs for Y2K[1]

In US$

Country	Estimated costs
Australia	398 mil. total, including supplementary 80 mil. (1998-1999)
Canada	703 mil.
Finland	18 mil.- 36 mil. per year (5-10% of yearly IT budget)
Hungary	46 mil.
Iceland	482,000 (1998-1999)
Ireland	75.6 mil./ year, including 17.6 mil. supplement (1998-1999)
Korea	78 mil. in 1998, 65 mil. for 1999
Mexico	300 mil. total
Netherlands	1.1 bil. total
Sweden	672 mil. +
Switzerland	67 mil. total
United Kingdom	671 mil. total
United States	5 bil. total, 2.4 bil. in fiscal year 1998, $1.3 billion in FY 1999

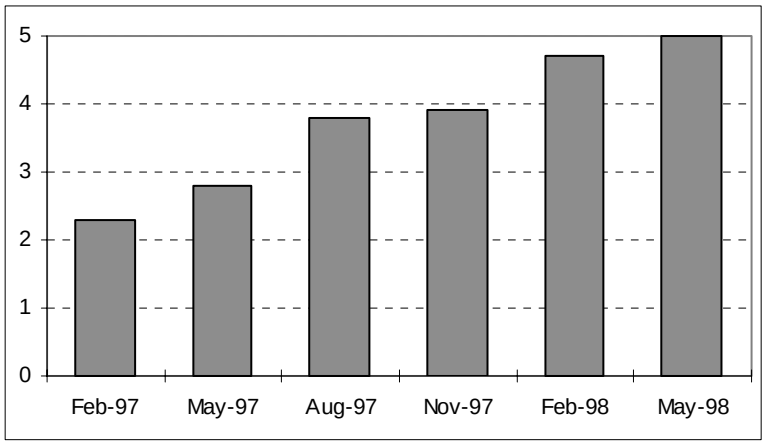
1. Figures are not strictly comparable.
Source: OECD.

79. Y2K costs are often initially underestimated by both firms and governments: in the *US*, the Office of Management and Budget (OMB) has been reporting periodically on *US* federal agencies' costs. The estimated total cost for the public sector has been continuously revised from US$ 2.3 bn in February

1997, to over US$ 5.0 in May 1998 (see Figure 1.1)[16]. These upward adjustments have been a common feature of most Year 2000 budgets in both public and private sector, as testing often accounts for more than 50 per cent of final costs.

Figure 1.1. United States OMB budget for Y2K repairs

Billions of current US$



Source: OMB (1997-98), various reports.

Other sectors

80. In addition to these "critical" sectors, a variety of other sectors could potentially suffer from Y2K-related failures which could spread to other parts of the economy: many manufacturing industries rely heavily on automated production facilities, wholesale and retail trade which use highly automated inventory and sales equipment. The UK Health and Safety Executive (HSE) has published specific guidance on safety-related control systems, and how Y2K-related failures could affect industrial installations (HSE, 1997 and 1998).

Global/international initiatives

81. Due to the serious danger of international disruption in areas such as foreign exchange markets, financial transactions, or air traffic, as well as the need to co-ordinate cross-border repairing and testing activities, and to exchange information, various international initiatives have been recently launched to deal with the issue. In June 1998, the United Nations issued Resolution 98-17104(E) calling on governments to co-operate on global awareness initiatives, and on public and private sectors to share experiences on solving the issue. The Information for Development programme of the World Bank (infoDev) has launched a special initiative to address the Y2K issue in developing countries. infoDev will provide technical assistance and organise regional workshops supported by a £10 million grant (US$16 million) from the United Kingdom government, while the US has also announced plans for $12 million in support. National leaders at the G8 summit in Birmingham in May, 1998 also announced

16. This figure does not include the Federal government's share of the costs for State information systems that support Federal programmes (OMB, 1998).

an intent to work together to address the problem, including development of a co-operative information exchange programme with Russia.

82. A variety of international co-ordinating bodies have also undertaken Y2K action:

- the Joint Year 2000 Council, established under the auspices of the BIS (see section on financial services);
- the European Commission through DG-III has been organising workshops and publishing various progress reports from Member States through a dedicated Web site (http://www.ispo.cec.be/y2keuro/year2000.htm);
- the International Council for Information Technology in Government Administration (ICA), a network of government IT officials, published a report in August 1997 with 22 recommendations for government action to address the Year 2000 problem, and organised a follow-up workshop in June 1998, co-sponsored by the G8 Government-On-Line pilot project;
- the International Telecommunication Union (ITU) has set up a Task Force to co-ordinate activities in the telecommunications sector. Ad-hoc sub-groups are being created to work on specific issues such as inter-carrier-testing (ITU, 1998);
- the World Customs Organisation (WCO) has been actively promoting the Year 2000 Problem at the WCO Information Management Sub-Committee. It has also published papers explaining the problem and describing the strategies of various customs administrations (http://www.wcoomd.org).

83. Some international industry groups have also taken a leading role in raising global awareness and co-ordinating international efforts: the World Information Technology and Services Alliance (WITSA) for the IT sector, Global 2000 for the banking industry, IATA for air transport, and the International Chamber of Commerce (ICC) for worldwide business organisations and firms. (See Annex A for a full list of World Wide Web sites from Member countries and international organisations)

Economy-wide effects:

84. Although detailed cost estimates are available from large corporations in some OECD countries[17], few estimates on nation-wide costs and possible macro-economic effects have been published. Most studies have concentrated on the direct costs of fixing the problem, mainly because it is easier to estimate this than the probability and effects of non-compliance. However, as noted previously, the most significant effects on overall economic growth would come from service interruptions caused by non-compliance, rather than from the direct spending on fixing the problem. Economy-wide costs are usually based on either an estimation of lines of codes to be fixed (or similar software metrics), or by extrapolating from a known number of large firms (usually based on turnover or a similar measure of relative economic importance -- see Annex Table 1). These estimates are inevitably subject to wide margins of error due to the general uncertainty about completion schedules and the reliability of testing

17. An example is Edward Yardeni's Y2K Disclosure Project for US S&P 500 corporations, an on-line database of Y2K disclosure statements : http://www.progsys.com/yardeni/y2kfind.asp

procedures, but provide a useful measure of the relative importance of the problem for both the public and private sectors.

85. The most widely quoted figure for world-wide costs is that of the Gartner Group which has estimated that the cost of a global fix could reach US $300-600 bn. This estimate is based on cost per line of code and excludes both consequential disruption losses and chip replacement costs. A much higher figure is that of Software Productivity Research (SPR, 1997) who estimates a total world-wide cost of US$ 1.6 trillion, including (among others) US$ 530 bn for initial software repairs, US$ 454 bn for database repairs, US$ 300 bn for litigation/damages, and US$ 76 for hardware chip replacements[18]. The US Fed has estimated that the total world-wide repair could cost US$ 300 bn (see Annex Table 1).

86. A second and more important measure of the relative economic importance of Y2K is the estimate of the cost of non-compliance, and how this cost translates into disruption at a macroeconomic level. Estimates of macroeconomic effects are based on assumptions about how economy-wide costs are treated (estimates of spending), estimates of how many systems or firms could fail, as well as assessments of how severe the damage could be from non-compliance in main infrastructural sectors (estimates of lost output). Given the high degree of uncertainty about these underlying (and often unstated) assumptions, as well as the lack of a solid analytical framework to assess the impact of these assumptions, few analysts have attempted to forecast the macroeconomic effects of Y2K[19]. Nevertheless, some initial studies have been conducted for Canada, Korea[20], the Netherlands, the United Kingdom and the United States. Among the main areas of concern highlighted in most studies are:

- short-term inflationary pressures in countries close to their peak in the economic cycle due to demand for new investment, supply-side disruptions, and significant wage increases;
- negative reactions from financial markets as the level of Y2K-related risk of firms and countries becomes more apparent;
- possible declines in productivity growth, and;
- a transitory drop in output due to a significant number of failures in critical information systems throughout the economy.

Country surveys

87. A report by the Bank of Montreal (Bank of Montreal, 1998) gives a broad overview of the main issues. Depending on the treatment of Y2K reprogramming expenditure by statistical agencies, Y2K could foreseeably have a positive short-term effect on real GDP during 1996-99. The report argues that if

18. Software Productivity Research's estimate is based on "function point" metrics which are considered by some industry experts to be a more reliable measurement of software complexity than lines of code. Function point counts are based on a variety of attributes of computer languages and applications such as inputs, outputs, enquiries, logical files and interfaces.

19. Governor Edward W. Kelly Jr. of the United States Federal Reserve Board declared at a US Senate hearing that "it is impossible to forecast the impact of this event, and the range of possibilities runs from minimal to extremely serious." (28 April testimony).

20. In June 1998, the Korean government reported to the OECD Secretariat that it expected a 0.4% drop in GDP growth because of the Year 2000 Problem (OECD questionnaire).

most of the firms' costs relate to programming (which would be counted as wage and salary expenditure, given the labour-intensive nature of the fix), this could potentially translate into inflationary pressures, given the tightness of the IT labour market. If on the other hand, Y2K expenditures relate to investment, future measures of capital and multifactor productivity would decline, given that output is not increasing. In the case of *Canada*, programming costs are not expected to reduce growth by more than 0.4 % in any one year between 1996-99.

88. In May 1998, ING Barings Research published the results of an extensive survey highlighting the risks that the Dutch economy faces due to Y2K (ING Barings, 1998). The main assumptions for their estimates (which are made on the basis of a "cautious" scenario) are:

- the effects of Y2K in the Netherlands will be typical of those in other EMU member states, as well as the United States and Japan;
- a two-month loss of industrial production in early 2000 in 20% of all businesses (except for those in the primary sector) translates into an economy-wide loss of production averaging 1.5%, with the government and large parts of the public sector generally unharmed;
- possible delays in payments of salaries and benefits as well as undermined consumer confidence could reduce private consumption by 0.25% below the baseline;
- 5% extra demand for business services (including, but not limited to, IT services);
- a 2% slowdown in global trade and in Dutch exports.

89. ING Barings calculates changes in sales at a sectoral level, and through the use of input-output tables, estimates the effects of these changes on primary cost categories (imports, wages, indirect taxes, profits). Table 1.7 summarises the main impacts on the Dutch economy for the year 2000 according to ING Barings' model.

Table 1.7. Macroeconomic effects of Y2K on the Netherlands' economy

Change from baseline scenario in percentage

Category	Change in percentage
Private consumption	-0.7
Government consumption	0.0
Capital spending	1.5
Exports	-3.6
Sales	-1.4
Imports	-2.0
National income (net at factor costs)	-1.1
out of which:	
Wages and salaries	-0.9
Income from dividends and business earnings	-1.4
Indirect levies less subsidies	-0.6

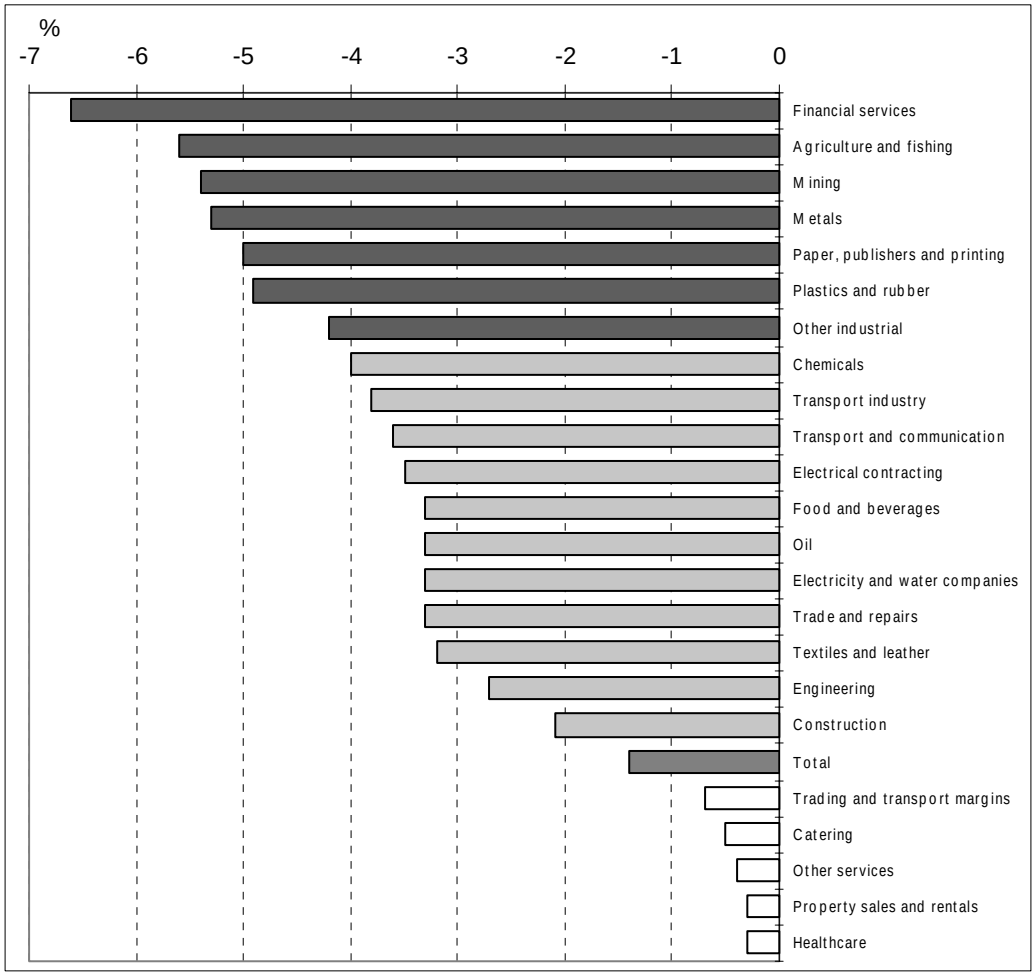
Source: ING Barings (1998)

90. In addition, this study estimates the relative decline of final demand (see Figure 1.2) and earnings. The industries where profitability will potentially be the hardest hit (more than 3.5%) are basic industry (mechanical engineering, rubber, chemicals and textiles), food, drink and tobacco, and the vehicles and transport equipment industry.

91. The study concludes that although the scenario used is a cautious one assuming relatively high degrees of compliance, the resulting production loss of 1.5% due to underestimation of the problem by the private sector (or flawed repairs) could foreseeably result in stagflation, unemployment and budgetary tensions.

Figure 1.2. Impact of Y2K on final demand in the Netherlands by sector, 2000

As a percentage of final demand according to baseline scenario



Source: ING Barings (1998)

92. A study of the *United Kingdom* economy by Dresdner Kleinwort Benson (DKB) concludes that growth due to increased spending on Y2K fixes is quickly offset by lost output from early system failures (UK Treasury, 1998). According to the report, by the year 2000, output could drop by more than 1% due to a large number of non-compliant systems, but growth would resume by the next year resulting in an total decline in GDP growth of 0.5% over the three years to 2001.

93. Several studies have focused on the *United States*, where the absolute impact could arguably be the largest given the size of the economy and its heavy reliance on IT. In April 1998, Governor Edward Kelly of the Federal Reserve Board at a Senate testimony announced that the Y2K problem could shave 0.1% annually off US real GDP for the following 2 years; and 0.1 to 0.2% off labour productivity growth.

Another assessment from DRI forecasts a decline in 1999 GDP growth of 0.3% and 0.5% in 2000 and 2001 due to increased inflation (+0.4%) and lower productivity. The total cost is estimated at US$ 119 bn, or 1.5% of GDP due to lost economic output. Goldman Sachs estimates that the Y2K cost will be equivalent to around 0.15-0.60% of GDP annually between 1997-2000. According to their assessment, the following main economic repercussions could be anticipated:

- economic activity will be boosted in the short-run: since spending on hardware is counted as capital spending, any Y2K hardware related spending will be reflected in growth of GDP;

- a decline in productivity growth as part of the expenditure is used to maintain the economy's current productive capacity, rather than to augment it; and temporary increases in employment (such as consultancy work to repair code) are not followed by an immediate effect on output;

- upward wage pressure as demand for IT specialists increases, and potential labour inflows from developing countries would not absorb a sufficient part of programming needs;

- reduction of corporate profits for firms operating in competitive markets or inflationary pressures due to companies in sectors facing excess demand passing Y2K costs along to customers through higher prices; and

- financial market reaction related to a potential Y2K risk premium: stock prices should reflect the extent of a company's fixes, as well as the probability of lower earnings, or even bankruptcy. Possibility of a "flight-to-quality" into United States assets.

94. A far more pessimistic assessment comes from the chief economist of Deutsche Bank Securities, Edward Yardeni, who argues that given the insufficient international leadership, the slow pace of repairs in the government sector, and the serious lack of information on progress outside the US, the chance of a serious global recession (as severe as the 1973-74 downturn during which real US GDP dropped 3.7%) could be as high as 70%. An identical drop, starting in 2000, would reduce real GDP by US$300 billion, back to where it was in early 1998. Yardeni argues that a deflationary recession is possible, with prices in the US dropping by as much as 5%, and a potential decline of nominal US GDP of up to US$ 1 trillion. (http://www.yardeni.com)

95. A recent study by Oxford Economic Forecasting (OEF, 1998) predicts that advanced economies may suffer a permanent loss of output of around 0.3% of GDP annually due to the Year 2000 problem. This study assumes that less than 30% of spending on repairs is productive in any sense other than fixing the problem. This reduction of productive potential is expected to have small adverse effects on output (between -0.2 and -0.3% of GDP annually for the G3 countries and the United Kingdom) and on inflation since spare capacity is reduced, putting upward pressure on prices (between 0.1 and 0.2% increase in consumer prices for these countries). The study confirms the speculative nature of any estimates of the economy-wide disruptive effects of Y2K, and concludes that given *a)* the strong incentives for firms to complete their repairs on time, and *b)* the outcomes of similar past disruptions where the impact on GDP growth was overestimated, the total short-term impact is unlikely to be more than 0.5% of GDP for the first quarter of 2000.

Overall impact

96. It should be noted that some of these estimates are based on pessimistic assumptions about the progress of remediation activities and should be viewed with caution. It is clear that although the overall effect of Y2K will be negative in the short-run, positive outcomes should be expected in the medium-term as Y2K offers an opportunity for firms and governments to review their IT portfolios, replace outdated systems, and enhance the future productivity of their investments. It appears that a significant share of expenditures will involve moving forward investments which in many cases would have taken place in any case at a later stage.

97. However, OECD countries could also suffer negative effects from non-compliance of trading partners, given their global economic interdependence. Although the quality of the data is erratic, industry experts feel that a major impact could come from disruptions in Asia where the currency and financial crisis has slowed down Y2K remediation efforts[21]: Indonesia and China are consistently identified as particularly vulnerable countries, and to a lesser extent, Malaysia, Thailand and the Philippines.

98. The degree of uncertainty on the pace of repairs and testing activities, and the lack of a clear picture on the global status of governments and firms makes economic forecasting of Y2K a particularly challenging exercise. Nevertheless, it appears from current data, that even lower range estimates would indicate potentially significant economic impacts. Even if the probability of worst-case scenarios is relatively low, the potential for major disruptions should not be underestimated or overlooked. As described in the next chapter, governments are clearly concerned and have begun taking action to address the Y2K challenge.

21. Merrill Lynch has recently completed a survey of thousands of companies world-wide which indicates that less than two-thirds of Asian firms expect to be Y2K compliant on time (Merrill Lynch, 1998).

Annex Table 1. Estimates of Y2K fix costs

Country / coverage	Estimate (bn of US$)	Source	Date	1997 IT market (bn of US$)	1997 GDP (bn of US$)
Worldwide	300-1600			703.9	
Total including litigation	1600	Software Productivity Research	Jan-97		
Software repairs	300-600	Gartner Group			
Software repairs	530	Software Productivity Research	Jan-97		
Total	300	US Fed	Apr-98		
Hardware chip replacements	76	Software Productivity Research	Jan-97		
OECD					
Total OECD	1200	Cap Gemini	Apr-98		
12 OECD countries	800	Cap Gemini	Apr-98		
United States	95-520			293.9	8 080
Total	520	Cap Gemini	Apr-98		
Total	240	Harris Bank / Bank of Montreal	Apr-98		
Total	150-200	Gartner Group			
Total	119	DRI	Mar-98		
Total	115	International Data Corp.			
Total	95	Goldman Sachs	Jun-98		
Software repairs only	74.6	Software Productivity Research	Jan-97		
Private sector	50	US Fed	Apr-98		
Largest 250 firms	37	Triaxsys Research	Apr-98		
Fortune 500 firms	11 [1]	US Fed	Apr-98		
Public sector	5.0	OMB	Jun-98		
Canada					618
Total	30	The Financial Post	Jul-97		
Total	15.3 [2]	Bank of Montreal	Apr-98		
Total	8.7	Conference Board of Canada			
Total public sector	0.7	Braiter/Westcott Report	Feb-98		
Asia-Pacific					
Australia	10	Newsbytes	Dec-97		393
Australia	4.1	Coopers & Lybrand	Nov-97		393
Korea	2.7	Korean Govt.	Jun-98		443
New Zealand	1	Sunday Star - Times	Jan-97		65

Annex Table 1. Estimates of Y2K fix costs (continued)

Country / coverage	Estimate (bn of US$)	Source	Date	1997 IT market (bn of US$)	1997 GDP (bn of US$)
Europe					
11 European countries	197	Cap Gemini	Apr-98	181.3	
Total private sector	100	PA Consulting Group	Mar-98		
Germany	88	Cap Gemini	Apr-98	48.4	2 100
United Kingdom	51.7	Taskforce 2000		35.7	1 287
United Kingdom	51	Cap Gemini	Apr-98	35.7	1 287
United Kingdom	16.7	Richard Holway		35.7	1 287
Italy	16	Cap Gemini	Apr-98	16.9	1 145
France	12	Cap Gemini	Apr-98	36.0	1 395
Belgium	12	Internat. Market Insight Reports	Feb-98	5.9	242
Netherlands	9.8	PA Consulting		10.7	361
Netherlands	9	Cap Gemini	Apr-98	10.7	361
Netherlands public sector	1.1	OECD questionnaire	Jun-98		
Belgium	6	Cap Gemini	Apr-98	5.9	242
Sweden	6	Cap Gemini	Apr-98	8.1	228
Norway	3	Cap Gemini	Apr-98	3.8	153
Spain	3	Cap Gemini	Apr-98	7.8	531
Finland	3	Cap Gemini	Apr-98	3.1	119
Denmark	1	Cap Gemini	Apr-98	4.9	170

1. Only 168 firms reporting.
2. Extrapolated from Stats Canada survey.

Source: various sources, including EITO (1998) for IT markets.

PART II: GOVERNMENTS' ROLE AND ACTIONS

99. Responding effectively to the "Year 2000 Problem" poses a major public management challenge for governments, requiring efforts to to assess and understand the extent of the problem, to develop appropriate policy responses, to establish mission-critical priorities, to raise awareness and motivate action, and to co-ordinate and implement action plans. As US President Bill Clinton recently stated, "With millions of hours needed to rewrite billions of lines of code, and hundreds of thousands of interdependent organisations, this is clearly one of the most complex management challenges in history. "[22]

100. The introduction to this report sets out the scope of the problem and the particular importance of government as both a large user of IT systems within the economy, and potentially as a leader in raising awareness and establishing policy-frameworks for addressing the problem. This chapter examines how governments are facing these challenges within the public sector, and how they are attempting to promote preparedeness society-wide. The report concludes by suggesting areas of continuing concern where further action is necessary.

Governments' Assessment of the Year 2000 Problem

101. An overall review of government responses to the OECD questionnaire suggests that most of those governments responding are well aware of the problem and have embarked on a wide range of efforts aiming to address public sector readiness and to raise awareness throughout their economies. Nearly every country responding has created or designated one or more national co-ordinating and/or awareness-raising institutions, and nearly all have begun assessing and reporting on progress.

102. However, as noted in the introduction to this report, there are also reasons for concern about how prepared governments will actually be when the Year 2000 arrives. A number of governments have only recently initiated or considered such programmes, and most governments either could not or chose not to provide hard, quantitative data on the extent of the public sector's compliance at this stage. Even in countries that appear to have major and highly publicised efforts going on at multiple levels, concerns are frequently raised by the media, private sector consultants and Y2K specialists about whether preparations are progressing adequately. Those results that are available on public sector progress suggest that some government agencies continue to lag and that a tremendous amount remains to be done.

103. Most governments have not developed comprehensive assessments of how the Year 2000 Problem will impact their economies. A minority (eight) indicated that they have developed whole or partial estimates of national, economy-wide impacts. Because of great uncertainty regarding how effective prevention efforts will turn out to be, even fewer have actually developed quantified estimates of impacts *(Canada, Korea, Netherlands*, details provided in Part I, pars. 87-95).

22. From July 13, 1998 Clinton speech on the Year 2000 Problem given at the National Academy of Sciences.

104. Short of overall economic assessments, some governments have attempted to take a comprehensive look at the problem through more qualitative assessment by sector, surveying the private sector regarding levels of awareness and readiness, and developing worst-case and best-case scenarios. These worst-case or disaster scenarios, as commonly reported in the media, can be seen as a motivating force for action.

105. On the other hand, concern also is expressed that overly "alarmist" or "sky-is-falling" scenarios could prompt public feelings of helplessness or even panic that could cause greater damage than the problem itself. To mention some common examples, consumers could create shortages of cash, food or other supplies if, due to lack of confidence in the technical infrastructures that support these sectors, they withdraw large sums of cash and stock up on supplies in preparation for the new millennium. If there is little confidence in airline safety and the vast majority of the public refuses to fly as a result, airlines may face a problem of lack of capacity at airports to accommodate their grounded aircraft fleets. The media have reported a growing backlash against disaster scenarios, prompting some to dismiss the existence of a serious problem altogether.

106. Such concerns suggest that periodic, measured government assessments, involving review of actions and readiness sector by sector, provide a more credible approach to motivating action and building public confidence that remedial action is going forward. Reports by *Canada, New Zealand, UK* and *US,* referred to in Part I, par. 24 of this report, provide good examples of this approach.

107. Within the public sector itself, governments have clearly undertaken more detailed assessments of preparedness and costs, though many governments nevertheless have had difficulty measuring and quantifying the overall costs they will face in addressing the Year 2000 problem (as noted in Part I, par. 77). A common approach taken to assessing the extent of the problem is to conduct a government-wide risk analysis that identifies what systems are most vulnerable to failure and most "mission-critical," either directly for government operations or more broadly for the economy as a whole. Thirteen countries reported undertaking government-wide risk assessment initiatives. For example:

- *Australia's* Commonwealth Government's risk assessment identified payments, social welfare, employment, defence and national security, health and revenue collection as the highest priorities for achieving compliance.

- *Iceland* reports that its risk assessment of government institutions determined that the problem will be "well under control, and risk of major disruptions in government operations is very low."

- The *Republic of Korea* is taking a more quantitative approach to risk assessment. According to the government's April, 1998 national assessment of readiness, 21% of hardware and 26.7% of software may cause problems.

- *Netherlands* is conducting a national risk analysis dealing with vital sectors and vital supply chains, the auditing of Year 2000 projects in vital sectors, welfare consequences of Year 2000 failures and the human behaviour anticipated if specific combinations of vital sectors fail. The results will be used for prioritising as well as contingency planning.

- *Sweden* reports continuous use of risk assessment, conducted through the Statskontoret's (Swedish Agency for Administrative Development) monitoring and evaluation of agencies. Central government agencies will undertake risk assessments of their most critical infrastructures.

Policies and Priorities for Addressing the Problem

108. **The role of government.** All 26 OECD countries responding to the questionnaire agreed that the government has a role to play beyond simply its own operations, in raising public awareness regarding the scope of the problem and the need for it to be addressed. Most countries have established public sector, private sector and/or joint public-private task forces to assist in this task. At least 20 OECD countries promote educational efforts through government-sponsored information available on the World Wide Web (list in Annex A). While there is a recognition across all countries that the private sector must ultimately be responsible for ensuring its own preparedness, certain governments seem to be taking more aggressive action in ensuring awareness and promoting action beyond the government sector, including subsidising private sector action. For example:

- *Australia*, like many other countries, has established public sector and private sector task forces to promote and co-ordinate action. They have also gone a step further by allowing favourable tax treatment for businesses, which can designate Year 2000 remediation expenses as current rather than capital expenses. *Australia* also recently launched a US$6.7 million television advertising campaign, targeted particularly at raising small business awareness.

- *Canada* has established multiple institutions to promote awareness and action across the economy: a government-industry task force was established in 1997 under the Ministry of Industry to bring together representatives of key sectors of the economy; its Year 2000 Project Office oversees public sector preparedness; and the Department of Foreign Affairs and International Trade monitors international readiness and has established a Year 2000 discussion group for Foreign Ministries. The government has also announced tax relief for small businesses in the form of accelerated capital cost allowances (over one year instead of six) for Year 2000 repairs.

- *Japan's* Development Bank and Finance Corporation for Small Business are providing low-interest loans in support of industry preparations. Loan guarantees and tax reductions for Y2K-related expenditures are also being offered to the private sector. Awareness-raising has included the Ministry of International Trade and Industry briefing sessions for a variety of business organisations, and Small Business Promotion Corporation seminars for small and medium businesses in more than 90 locations.

- *Korea's* government has promoted private sector action by conducting seminars and workshops, a national media campaign, and by setting aside US$23 million in funding for the issuance of government-sponsored loans to an estimated 1 500 small and medium businesses in 1998. Korea cites the government's role as particularly important to help overcome the effects of recent economic difficulties there.

- *Netherlands*, through its National Millennium Platform, a joint public-private sector task force with a US$6.5 million two-year budget, is actively promoting awareness and initiating actions through a series of pilot projects across the economy, aimed at developing solutions to technical, legal and other issues.

- With Prime Minister Tony Blair taking the lead in public speeches, *United Kingdom* has moved aggressively through its US$26.7-million Action 2000 task force and policies to fund small business preparations to address the Year 2000 problem. *UK* has particularly emphasised the need for international preparations, conducting preparedness surveys through

all of its embassies, contributing US$16.7 million to the World Bank to support government efforts in developing countries, and US$25 000 to supplement OECD work in this area. Inland Revenue's Tax Bulletin has also confirmed that corporate expenditures on millennium compliance qualify for tax relief.

– *United States* has established a "President's Council on Year 2000 Conversion," comprised of high-level representatives of 35 Federal agencies and headed by a full-time "Year 2000 Czar," whose role it is to promote national and international awareness. The agencies are chairing working groups involving industry trade associations from 32 sectors, with particular priority given to working groups involving key infrastructure areas of energy, telecommunications, financial institutions, emergency preparedness and workforce issues. The U.S. is also contributing $12 million to the World Bank for Y2K assistance to developing countries.

109. While these countries' actions in themselves do not ensure that their economies will be ready when the Year 2000 arrives, their transparent approach and adoption of specific policies singling out the problem as a particular national concern would appear to provide additional impetus for preparations to progress across the economy.

110. On the other hand, a number of countries suggest that while the government should play a role in promoting awareness and action in the private sector, the government has relatively weak leverage to ensure this occurs. These countries (e.g. *France, Germany, New Zealand*) tend to place greater emphasis on the responsibilities of the sectors themselves to address the problem.

111. **Economy-wide priorities.** A majority of OECD governments cite explicit policies giving priority to preparations in particular sectors. The energy sector, communications, financial sector, transportation (including air, rail and road safety), health services and supply of water are most consistently mentioned as among top national priorities.

Table 2.1 Sample of Government Y2K Priorities by Sector

Question: Does the policy establish priorities for addressing specific sectors of the economy?
(e.g. communications, emergency services, energy, finance, transport, utilities);
If yes, what are these priority areas?

	Australia	Canada	Finland	Iceland	Italy	Japan	Korea	Mexico	Norway	Netherlands	Spain	Sweden	Switzerland	United States
1. Major Sectoral Priorities														
Energy	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Communications	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Financial	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔
Transportation	✔		✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Health	✔		✔	✔	✔	✔	✔	✔	✔	✔		✔		✔
Water	✔			✔				✔		✔	✔	✔	✔	✔
2. Government Sectoral Priorities														
Defense	✔				✔				✔	✔				
Disaster Management		✔								✔				
Judicial System										✔				
Welfare & Pension Payments	✔							✔		✔				
Postal Services												✔		
Revenues & Tax Collection	✔							✔		✔				
3. Local Level														
Emergency Services	✔	✔										✔	✔	✔
Police					✔				✔	✔				✔
Municipal Services	✔													
4. Others														
Small-and-Medium Enterprises	✔						✔				✔			✔
Food Supplies								✔		✔				✔
Shipping							✔		✔			✔		
Industrial Facilities							✔		✔		✔			
Consumers & Users											✔			
Environment											✔			
Insurance					✔									
Construction									✔					
Retail									✔					

Source: Responses to "Enquiry and Description of OECD on the Y2K Problem/ Millennium Bug", June 1998.

112. Moving from economy-wide concerns to the operation of the public sector itself, governments were less inclined to single out priority sectors, usually suggesting that each ministry should identify its mission-critical systems and priorities. Another approach, taken by *Canada*, was to identify 48 government-wide mission critical functions that impact on health, security and economic well-being as a focus of special attention.

113. Those governments that did mention priorities within the government sector cited defence, disaster management, the judicial system, welfare and pension payments, tax collection, postal services, police, emergency services, and municipal services generally.

Institutions for Co-ordinating Action and Awareness

114. All countries responding to the survey have assigned responsibilities for action on the Year 2000, and nearly all have specifically established one or more national Year 2000 bodies with responsibilities for co-ordinating action and raising awareness. In many cases, the oversight body is an existing agency or agencies within the government, but it can also be an interministerial task force, or a joint public-private sector task force. While some countries have appointed a Y2K "czar" as public spokesperson on the problem, most countries are finding that the problem is so omnipresent and wide-ranging in its impacts that it is necessary to establish multiple points of responsibility (see Table 2.2).

115. For example, *Australia, Belgium, Canada, Denmark, France, Sweden, Switzerland* and the *United Kingdom* have all split up responsibilities between an entity with broad responsibilities for raising awareness and supporting economy-wide efforts (*Australia's Year 2000 National Strategy, Belgium's Millennium Forum 2000, Canada's Year 2000 Task Force, Denmark's Year 2000 Forum, France's Commission Thery ("Passage informatique à l'an 2000"), Sweden's Millennium Commission, Switzerland's Year 2000 Delegate,* and *UK's Action 2000);* and a co-ordinating body within government for ensuring or supporting public sector readiness (*Australia's Year 2000 Project Office, Belgium's Admi-2000 Programme, Canada's Year 2000 Project Office, Denmark's Ministry of Research and IT, France's Commission Marchat, Swedish Agency for Administrative Development, Switzerland's Jahr 2000 Ausschuss,* and the *UK's Year 2000 Team).*

116. Responsibilities between co-ordination of action in the public sector and general awareness-raising are frequently separated. For example, *Japan's Interministerial Conference on Year 2000* has met twice at Cabinet level to promote co-ordinated action, but awareness-raising is undertaken by each ministry and agency. In *New Zealand,* a committee convened by the Ministry of Commerce has been promoting awareness since 1996, while a *Year 2000 Task Force* was established more recently, reporting to a Ministerial Steering Group, to conduct surveys of progress and build on existing awareness-raising initiatives.

117. Other countries have established co-ordinating bodies with a more integrated, over-arching role *(Austria's Co-ordinating Commission for IT* within the *Federal Chancellery, Hungary's Government Committee for IT and Telecommunications, Mexico's National Commission for the Informatics Conversion Year 2000, Netherlands' National Millennium Platform,* and the *United States' President's Council on Year 2000 Conversion).* In addition to raising awareness, responsibilities include monitoring and assessing progress, offering of support, and co-ordinating action.

118. Some governments have sought to integrate Year 2000 planning into their normal operating functions without establishing an interministerial or public-private sector task force. For example, the *Czech Republic's* Office for State Information Systems conducted a government-wide survey of readiness in April, but decentralised units have generally been established in each central state authority to address the Year 2000 problem. *Finland,* while recently establishing an interministerial working group to address interoperability issues and data exchange, also primarily handles oversight responsibility through its existing management and budget structure. *Germany* assigns responsibility for awareness-raising and interface with the private sector to its Ministry of Economic Affairs, while oversight of the public sector's

efforts is handled by the Ministry of Interior. *Iceland's* Ministry of Finance is working to build awareness throughout the public and private sectors through communications with government institutions, trade organisations, municipal authorities and the press. *Korea's Year 2000 Problem Council* within the Administrative Co-ordination Office maintains responsibility for administrative action and awareness-raising in the civil service, while the Ministry of Information and Communication is responsible for development of a national action plan and awareness-raising economy-wide.

Table 2.2 National Co-ordinating Bodies

Country	National Co-ordinating Bodies	Targeted Sector	Main Emphases			
			Awareness Education	Monitoring Oversight	Coordination Cooperation	Technical Advice
Australia	Year 2000 Project Office	Public Sector		✔		
	Year 2000 National Strategy	Private Sector	✔		✔	
Austria	Federal Chancellery-Coordinating Commission for IT	Public/Private	✔		✔	✔
Belgium	Forum 2000	Private	✔		✔	✔
	Admi-2000 Programme	Public		✔		
Canada	Year 2000 Project Office	Public	✔	✔	✔	
	Task Force	Private	✔	✔	✔	
Czech Rep.	Units created in each central state authority					
Denmark	Year 2000 Forum	Public/Private	✔		✔	✔
	Year 2000 Secretariat	Public	✔	✔	✔	✔
Finland	Interministerial Coordinating Group	Public			✔	✔
France	Commission Thery	Public/Private	✔			
	Commission Marchat	Public			✔	✔
Germany	Ministry of Economic Affairs	Private	✔		✔	
	Ministry of Interior	Public	✔		✔	
Hungary	Government Committee for IT & Telecommunication	Public	✔	✔	✔	✔
Iceland	Ministry of Finance	Public/Private	✔		✔	
Ireland	Interdepartmental Year 2000 Monitoring Committee	Public/Private	✔	✔		
	Dept. of Enterprise,Trade & Employment	Private	✔		✔	
Italy	Committee "Anno 2000" planned	Public/ Private	✔	✔	✔	✔
	L'Autorita per l'Informatizzazione della Publicca Amministrazione	Public	✔	✔	✔	✔
Japan	Inter-Ministerial Conference on Yr 2000	Public	✔		✔	
Korea	Year 2000 Problem Council	Public/Private	✔			
	Min. of Information & Communications	Public/Private	✔		✔	
	Min. of Gov't Adm.& Home Affairs	Public		✔		
Luxembourg	Interministerial group proposed, decision pending					
	Centre Informatique de l'Etat	Public	✔			
Mexico	National Commission for Conversion	Public/Private	✔			✔

(continued next page)

Table 2.2 National Co-ordinating Bodies (continued)

Country	National Co-ordinating Bodies	Targeted Sector	Main Emphases			
			Awareness Education	Monitoring Oversight	Coordination Cooperation	Technical Advice
Netherlands	National Millennium Platform	Public/Private	✔	✔	✔	✔
	Gov't Y2K Project Office	Public	✔	✔		
New-Zealand	Year 2000 Task Force	Public	✔			
Norway	Min. of Trade & Industry	Public/ Private	✔		✔	
	Action Year 2000 Unit	Public	✔		✔	
Poland	Min. of Interior and Administration		✔	✔		✔
	Co-ordinating Com. (Telecom and IT Dept.)					
Portugal	Intersectoral Committee for IT	Public/Private	✔		✔	✔
	(supported by Min. of Finance Informatics Institute)					
	Min. of Science & Tech. Mission Team	Public	✔	✔	✔	✔
Spain	Ministry of Public Administrations	Public	✔	✔	✔	✔
	National Commission	Public/Private	✔		✔	
Sweden	Millennium Commission	Public/Private	✔		✔	
	Agency for Admin. Development	Public	✔		✔	
Switzerland	Jahr 2000 Ausschuss	Public/Private	✔	✔	✔	✔
United	Year 2000 Team (Cabinet Office)	Public		✔	✔	
Kingdom	Action 2000	Private	✔			
United States	President's Council on Year 2000 Conversion	Public/Private	✔		✔	

119. More detailed descriptions of a few countries' experience illustrate how such efforts are being managed.

- *Australia* has created a "Year 2000 National Strategy" to co-ordinate activities, raise awareness and understanding, stimulate remedial action and facilitate contingency planning. Operating through its Year 2000 industry programme, the National Strategy is targeted particularly at small and medium enterprises. State and territory governments are responsible for monitoring sectors where they have jurisdiction, such as electricity, gas water, sewerage, transport, health and emergency services. Within the Commonwealth, agency chief executives are responsible for compliance, while progress is monitored through quarterly reports by the Year 2000 Project Office within the Commonwealth Office of Government Information Technology.

- *Belgium's* joint public-private approach involves the Millennium Forum 2000 to address problems economy-wide; and the Bureau Conseil ABC's ADMI-2000 programme to oversee public sector action. A January 1997 government circular required establishment of a "Madame or Monsieur 2000" for each governmental ministry or agency, to be co-ordinated through the ADMI-2000 programme. The Millennium Forum, whose mission is to sensitise and advise about the Year 2000 Problem in general and to concentrate on business in particular, has established four working groups: a group to analyse the problem and look at embedded systems in particular; a group charged with communication and co-ordination; a

group bringing together the IT sector; and a group providing general advice. A fifth group is planned to examine legal and liability issues.

- *France's* Ministry of Economy, Finance and Industry created in February, 1998 the Mission, "Passage informatique à l'an 2000," to more strongly mobilise action on a national level, including regional goverment offices responsible for working with industry, professional and trade associations, chambers of commerce and SMEs. The group aims to identify where action is lacking or at greatest risk, to exchange and disseminate best practices information, and to provide guidance on legal questions, training and remediation efforts. Meanwhile, the Commission Marchat focuses on public sector readiness. Initially created to address information system adaptation to the single European currency, it has broadened its scope to include Year 2000 issues. This interministerial group of IT officials shares information across the public sector at the central and decentralised level, and focuses particularly on technical questions such as system configurations and interoperability of networks.

- *Ireland's* Interdepartmental Year 2000 Monitoring Committee, chaired by the Ministry of Finance, monitors and oversees preparations in central government departments and offices. An interdepartmental Special Interest Group was also established to promote awareness in the civil service. Meanwhile, a Year 2000 National Committee, supported by the Department of Enterprise, Trade & Employment, chaired by the Minister for Science, Technology and Commerce and comprising representatives of business organisations and development agencies, hosted seven regional conferences on the issue in May and June. Its Y2K Enterprise Awareness campaign issued brochures and guidance to over 150 000 businesses in March 1997 and again in May 1998.

- *Mexico* launched a National Commission for the Informatics Conversion Year 2000 in June, 1998. The Commission brings together key government ministries (e.g., Defence, Foreign Affairs, Treasury, Energy, Commerce and Industrial Development, Internal Auditing and Administrative Development, Communications and Transportation, Education, Health) as well as representatives of the private sector, academic and informatics communities. Chaired by the President of the National Institute of Statistics, Geography and Informatics, the Commission will initially conduct a national survey in the private sector and derive recommendations for specific actions for each sector and type or size of organisation, aside from the financial sector, where action is being co-ordinated by Mexico's central bank, BANXICO. SECODAM, the government agency for internal auditing and administrative development, will continue to co-ordinate and oversee activities carried out by the Federal Government. The Secretariat for Commerce and Industrial Development will promote related actions in the private and social sectors.

120. **International Co-ordination.** Because national governments and national economies are dependent on the support of services with infrastructures and supply chains that span beyond national borders, such as electricity, telecommunications, transport and financial services, international co-ordination is an essential component of Year 2000 preparations. Within governments, ministries of foreign affairs are most often designated to co-ordinate and oversee international efforts, with national Year 2000 co-ordinating bodies also sometimes taking on this role.

121. However, cross-border issues are so complex and wide-ranging that it is often necessary for ministries or departments responsible for particular sectors to also become involved at the international level. For example, *Ireland* notes that it is particularly active on a sectoral level in addressing cross-border co-ordination in such areas as aviation, telecom, gas, transport and electricity. While *Japan's*

Ministry of Foreign Affairs handles most international contact, its Ministry of Finance is involved in international co-ordination issues involving the financial sector, through the Joint Year 2000 Council and Bank of International Settlements. International co-ordinating groups such as these have sprung up in most sectors where cross-border issues are of particular importance. These sectoral initiatives are discussed in greater detail in Part I of this report.

122. *Canada*, *United Kingdom* and *United States* appear to be giving particularly strong emphasis to preparations at an international level through surveys of other countries' readiness conducted by their foreign embassies, and *UK* and *US* contributions to the World Bank's infoDev fund to subsidise developing countries' efforts to address the Year 2000 problem.

Public Management approaches to effective implementation

123. Behind the proclamations and urgent calls for action lies the unglamorous but challenging task of actually reviewing and preparing the government's computer networks and other operating systems with embedded chips for the Year 2000. Problems are likely to arise with growing frequency by the beginning of 1999, when many systems that look forward a year will begin encountering problems. So little time is left and so much remains to do (re-programming of computer codes and testing of systems are especially time-consuming) that prioritisation focusing on mission-critical systems is essential.

124. Part of the challenge is technical in nature, and this section does not attempt to address these questions, such as how to test systems and embedded chips, as other reports are available on these subjects from Web sites and sources with greater technical expertise than the OECD brings to the subject.[23] However, the report does seek to shed light on some of the key public management issues involved, and on how OECD countries are addressing them. These include the kinds of reporting systems or other incentives governments establish to ensure progress; budgeting and human resource policies and approaches to ensure adequate resources; regulatory strategies to either spur action or eliminate barriers to achieving compliance; and contingency planning to address unforeseen or worst-case scenarios.

125. **Reporting on preparations and compliance.** All but a few countries responding to the OECD questionnaire said they had established systems of reporting on readiness from the various departments involved in reviewing and testing their systems (*Austria, Czech Republic, Germany, Hungary* and *Poland* were the exceptions). Most required regular reporting in the range of every two to six months. *Canada* and *Korea* indicated recent moves to monthly reporting. However, many governments do not make results public, and details of results were not readily available in most cases. Selected results[24], where available, are provided below in Table 2.3.

23. For example, see "Year 2000 Testing: A Global Perspective" from the Joint Year 2000 Council; "Year 2000 Computing Crisis: A Testing Guide" from the U.S. General Accounting Office; and the *UK* CCTA Web pages on embedded systems (http://www.ccta.gov.uk/mill/embed.htm).

24. These selected examples do not include all countries' publicly reported results. Results provided here were either summarised in government responses to the OECD questionnaire, or obtained via the World Wide Web, while others were more difficult to access or report upon due to language barriers.

Table 2.3 Results of selected OECD Member country reporting on Y2K preparations

Country	Reporting Date	Results
Australia	Jul. 1998	Percentages of government business critical systems that have been repaired and are being tested or fully back on line by sector: • 60% underlying delivery of health & national safety services; • 48% in social welfare and employment; • 33% in revenue collection; • 40% in national security, excluding defence; • 34% of business critical functions in defence. • From 15% to 30% of systems & functions have completed testing and are fully compliant in these categories.
Belgium [25] (Admi-2000)	Jun. 1998	• 175 full-time personnel (including about 25% hired externally) needed. • 32% of the work has been undertaken in survey of 41 public agencies. • 5 institutions indicated their systems are ready; • 8 completed from 40% to more than 80% of work, 12 between 20% & 40%; • 13 have completed less than 20% of preparations & 3 have yet to begin.
Canada (National Statistics)	Jul. 1998	• 70% of businesses are taking action; • 94% of medium-sized & large firms are now taking action; • Per cent of firms taking formal action has doubled from 9 % to 18%; • Per cent of large firms taking formal approach has grown from 48% to 67%; • Close to 1/3 of Canadian businesses indicated that their systems were ready which represents 19% of the survey population employment.
Denmark	Apr. 1998	• All ministries have established a Year 2000 project organisation; • Work on most vital systems has long been started & are expected ready within planned schedule; • No reporting has been received indicating special budget consequences; • Tasks will be managed by changing the order of priority within the existing budget.
Finland	Dec. 1997	• About 42% had completed study, 32% reported work in progress; 5% ready • About 32% reported had done nothing.
Japan	Dec. 1997	• 40% of 395 priority systems at the central government level were ready, with remainder scheduled to be so by end of 1999; • 85% of action on information systems at the prefectural level was concluded or underway; • One-third of action was concluded or underway for municipal-level IS. • 2.3 - 3.0 million person-months of labour will be needed to address the problem economy-wide, according to Japan Information Service Industry Association survey in Feb. 1998.

25. As of 12 June, 1998, 12 of 43 entities had not responded to the latest survey, generally smaller institutions representing about 10% of total work. For the totals above, results from the March, 1998 survey were incorporated for nine agencies, from December, 1997 for one entity, and 2 non-respondents were not included.

Table 2.3 Results of selected OECD Member country reporting on Y2K preparations (continued)

Country	Reporting Date	Results
Netherlands (Ministry of Interior survey) (National Millenium Platform)	Apr. 1998 Feb. 98	• 99% of objects within the public sector with a possible millenium problem have been identified; • 71% completed impact analysis; • 25% of vital objects identified as having a problem, and the process of solving these problems had begun on 68% of these; • 97% of all organisations were aware of the problem; • 68% had started a millennium project; Small-&- medium sized entreprises & some sectors (parts of local government and transport) need additional attention.
Norway	First quarter of 1998	• Growing awareness within government, with larger entities best prepared; • About 1/3 of agencies have established a Y2K project; • There is insufficent risk analysis & contingency plans & considerable need for external resources reported.
Spain	Mar. 31,1998	• 88% of state agencies completed inventories of their systems; • 80% completed a diagnosis; • 62% prepared impact analyses; • 44% started conversion projects; • 43% completed planning of repairs; • 32% initiated testing procedures; • Results are not yet available from the quarterly update of 15 July, 1998.
Sweden	Mar. 31, 1998	• "Severe disruptions in several vital public functions can not be excluded," according to survey covering 54 government agencies. • 13 agencies designated as "red-light", or due for special attention because they were lagging behind average; • 40 designated as "yellow-light", signifying no cause for special attention; • 1 received a "green-light" signifying all mission-critical systems were sound. • 10% of Swedish municipalities have yet to begin work, according to an Association of Local Authorities survey of 288 municipalities; • 25% of local authorities have not yet begun addressing embedded systems.
Switzerland	Jun. 1998	• External audit found great variances among departments at this stage of the project. • 50% of government IT systems have been partly or fully tested; • About 20% of IT systems will be shut down or replaced.
United States (Office of Management and Budget)	May 15, 1998	• 40% of the 7,336 mission-critical systems identified are now compliant; • 42% are being repaired; • 14% are being replaced; • 4% are being retired. • Several Cabinet agencies (Defense, Education, Energy, Health and Human Services, Transportation & Aid for International Development) were classified in a bottom tier -- "insufficient evidence of adequate progress" to meet the 31 March, 1999 goal for full compliance.

126. The results above suggest that countries certainly are making progress, but that they have a long way to go; every country reporting results has the majority of work still ahead of them.

127. The *US* provides a special case because the quarterly results reported to OMB are also used by the House Sub-Committee on Government Management, Information and Technology of the U.S. House of Representatives to develop agency "report cards" ranging from "A" to "F," including failing grades for six agencies. Though grades were based primarily on estimated completion dates for compliance of mission critical systems, they were also adjusted based on a review of where agencies stood in developing contingency plans, inventorying telecommunications systems, testing embedded systems, and inventorying and planning for external data exchange. The "report cards" ended up drawing greater attention from the media and criticism of government preparations than the original OMB announcement of results.

128. Such experience suggests that publication of results can and has been used to criticise government efforts, but that public scrutiny and heightened accountability has also served as a motivating force for action within both the public and private sectors, and has enhanced government credibility and support as progress has become evident over time.

129. Some countries warn against the establishment of comprehensive reporting systems requiring excessive detail on how every agency and business is addressing the problem. They suggest that assessment of private sector preparations in particular should be targeted to priority sectors, and random sampling should be considered to minimize information-collection burdens. As a general rule for both the public and private sector, excessively detailed information and frequent reporting requirements can diminish the reliability of the results, and risk a shift in resources from compliance to reporting efforts. On the other hand, some information-gathering is necessary in order for governments to be able to assess progress, vulnerabilities and priorities for further action.

Budgeting and human resource strategies

130. As noted in paragraph 77, many governments have had difficulty developing good estimates of the cost of addressing the Year 2000 problem (see Table 1.1, Part I). This is in part because most countries have adopted the general policy that agencies are responsible for addressing the problem within their existing budgets, diverting funds from other projects if necessary. An argument can be made for this approach, given that most government agencies have IT departments whose personnel can devote their time to Year 2000 remediation as a priority over development of new systems. Within the context of some "central" oversight to facilitate sharing of information, expertise and best practices across agencies and ensuring interoperability for exchange of data, agencies generally should be able to prioritise to meet their own budget needs.

131. From a strategic point of view, however, an argument could also be made that the government has an obligation to ensure that adequate funding and effort is under way, particularly in priority sectors. Some governments have opted for this approach, setting aside extra funding as *Australia* has done, "as a seed fund to encourage and accelerate existing remediation efforts in highly technically dependent agencies with mission critical systems." About half of responding countries suggested that they have developed budgeting policies specifically addressing Year 2000 preparations, usually involving diversion of funding from other purposes. A few cite policies of specifically setting aside supplementary public sector funding (*Australia, Ireland, Japan, Korea,* and the *Netherlands)*.

132. *Canada, Netherlands, Sweden* and the *U.S.* have suggested they could withhold portions of IT funding if agencies are not making sufficient progress. The *U.S.* has also suggested it will reserve part of its fiscal year 1999 emergency funding for Year 2000 problems in the event that this is needed.

133. Some countries also cite concerns about a skills shortage and their ability to retain qualified expertise as consulting and IT sector wages rise in response to increased demand. In response to these concerns, *Netherlands'* Millennium Platform brought together the government, the IT sector, the temporary staff sector, training institutions and the national employment organisation to sign a national charter to jointly tackle the problem. The policy aims to mobilise 10 000 people from such targeted areas as pensioners, people in early retirement and on reduced pay schemes, unemployed people and students. Government has sought to spur recruitment by removing legal obstacles that would otherwise require individuals on pensions or reduced pay schemes to give up their entitlements by attending training or accepting temporary employment. The IT industry has agreed to provide experienced supervision to the new recruits. *Canada*'s recruitment initiatives include development of immigration measures to simplify and accelerate entry of temporary workers in high-skilled occupations. The *U.S.* is aiming to bring retired programmers back into the work force with the help of the non-profit American Association of Retired Persons, and expansion of the Department of Labor's national job bank to include a separate Year 2000 employment data base.

Regulatory strategies

134. Whether a government issues special "Year 2000" regulations or directives often depends upon its administrative culture and the degree to which it relies upon such regulations or directives to ensure implementation of overall planning. For example, *Belgium, Denmark, Hungary, Korea, Portugal, Spain, Sweden* and the *U.S.* have all issued general policy directives detailing how the problem should be addressed government-wide. However, over half of responding countries said they had not established regulations to specifically address Year 2000 preparations. "Additional regulation has not been considered necessary for this problem," the *UK* noted. "Its solution depends on co-operation between individuals, companies and organisations."

135. A few countries have been particularly active in considering special Year 2000-related requirements:

- *Denmark* has issued a note in co-operation with the Association of State-Authorised Public Accountants and the Association of Registered Public Accountants requiring auditors to review business' "Year 2000 status." As part of their annual review of business' presentation of accounts, they are required to assess the future prospects of the business and to point out any problems they encounter to the management. *Denmark* also has issued a directive based on a paragraph in the budget specifying duties of reporting on Year 2000 plans and actions within all government-financed organisations.

- *Korea's* government will be required to purchase only products that are "Year 2000-compliant" beginning in the second half of 1998. Soon, enterprises will be obligated to certify that their products are "Year 2000-compliant" regardless of whether the government is purchasing them. The Administrative Co-ordination Office has issued "executive directions" to all government agencies, and was expecting enactment of a "related law" by July, 1998.

– *Netherlands'* Cabinet approved a "Millennium Review of New Legislation" in December, 1997 which states that each minister has the obligation to verify that the effects of new legislation will not adversely affect efforts to address the Year 2000 problem. If these effects exist, a delay in the legislation or its operational effects should be considered. The "millennium review" has already resulted in the delay of some non-essential legislation in the area of social security.

136. *Denmark, Netherlands* and *Sweden* have supplemented their initiatives through voluntary approaches involving the IT sector's development of self-certification schemes. The aim is to provide buyers with a guarantee that the product is "millennium-proof" by giving them a written statement under which conditions the product has no millennium problem. There are limits, however, to such assurances, given that products may not achieve the same results when used in association with differing systems, software and operating conditions.

Information disclosure and liability issues

137. Product and company liability for Y2K compliance is a complex area, with little consensus about how best to address it. Concerns are frequently raised that information disclosure in the private sector is less than complete, due to business fears that they will be legally liable if they give incorrect information or reveal that they were aware of non-compliance and subsequently did not exert due diligence to address the problem. On the other hand, relaxation of liability for product compliance could risk undermining incentives for companies to address the problem. The *United States* in July proposed "Good Samaritan" legislation seeking to ensure that businesses that share information about the Year 2000 problem cannot be held liable if it is inaccurate. The law is being sought to encourage businesses that have difficulties with compliance of their systems or products to share this information, rather than keeping it secret to minimise risk of legal liability for Year 2000 failures. The *U.S.* Department of Justice in a letter opinion stated that competitors who merely share information about the Y2K problem are not in violation of antitrust laws.

138. The US Securities and Exchange Commission (SEC) amended its *Staff Legal Bulletin No 5 (CF/IM)* in January 1998 to impose new Y2K-related disclosure requirements. It concluded that "if the Year 2000 issues are determined to be material, without regard to countervailing circumstances, the nature and potential impact of the Year 2000 issues as well as the countervailing circumstances should be disclosed" (SEC, 1998*a*)[26]. In particular the following topics should be addressed in a "reasonably specific and meaningful" way:

– the company's general plans to address the Year 2000 issues relating to its business, its operations (including operating systems) and, if material, its relationships with customers, suppliers, and other constituents; and its timetable for carrying out those plans;

– and the total dollar amount that the company estimates will be spent to remediate its Year 2000 issues, if such amount is expected to be material to the company's business, operations or financial condition, and any material impact these expenditures are expected to have on a company's results of operations, liquidity and capital resources.

26. In general, "material" information encompasses information regarding any event which could alter a corporation's revenues, assets, or profits by 5 per cent or more.

139. The SEC has recently extended these requirements to investment advisers, investment companies, and municipal securities issuers (SEC, 1998*b*). Other stock exchanges such as the *Australian* Stock Exchange (ASX) and the *New Zealand* Stock Exchange (NZSE) have recently launched similar initiatives requiring listed firms to disclose Y2K activities and anticipated costs.

Contingency planning

140. Regardless of how well national governments prepare to ensure that their own operations are Year 2000 compliant, they will remain dependent on electricity, telephone systems, transportation and supply systems to continue functioning beyond the Year 2000. For these reasons, as well as the virtual impossibility of ensuring that their own systems are "Millennium bug-proof," preparation of contingency plans should be a critical component of every agency's preparations.

141. Contingency planning involves a disciplined investigation into all aspects of an agency's activities to locate those functions where significant risk exists that could immobilise the agency's ability to function. By identifying and assessing where its greatest risks exist, and developing plans for how they can continue to undertake mission-critical activities even in the face of particular system failures, agencies can be better prepared to address Year 2000 problems as they arise.[27]

142. About half of Member governments had already begun contingency planning, while some others indicated plans to do so by late 1998 or early 1999. Given the potential for many systems to break down or malfunction well before 2000, as they begin looking one year or more ahead, governments take significant risks by leaving contingency planning to the last minute.

27. For more information on contingency planning, see, for example, "Year 2000 Computing Crisis: Business Continuity and Contingency Planning," from the *U.S.* General Accounting Office (http://www.gao.gov/special.pubs/bcpguide.pdf);

CONCLUSIONS AND ONGOING CONCERNS

143. A review of experience within OECD countries, reports on various aspects of the issues, and the recommendations of a number of international organisations and associations (see Annex D), suggests a growing consensus for action to address the Year 2000 problem. A description of the OECD's own internal Year 2000 initiative also provides an example of an overall organisational approach to the problem (Annex E). While not every country is lagging in the areas highlighted below, there is reason for concern in many countries, and a need for sustained action in the following areas:

A Stronger Role for Governments

1) **Governments need to accelerate their own preparations.** Even governments that are often cited as world leaders in addressing the Year 2000 problem generally indicate that they have done **less than half** of the work required to achieve public sector compliance. This is particularly worrisome in light of many experts' view that systems ideally should be ready by the end of 1998, in order to avoid early manifestations of the Year 2000 problem in 1999. While work in most OECD countries is well under way, testing, the most resource-intensive and time-consuming phase of preparations, is only just beginning in many government agencies. Unable to complete all of the necessary preparations, governments are having to target mission-critical systems, leaving a large amount of work involving less critical systems for after the century date change.

2) **Governments have an important leadership role to play in promoting economy-wide preparedness.** Whether through policy actions, co-operative problem-solving with the private sector, or the more common emphasis on awareness-raising and information provision, governments can and must help to ensure that their economies are prepared for the Year 2000. Because the Year 2000 problem affects virtually every sector of society and because so many interdependencies exist, government action to promote overall readiness is commonly accepted and broadly supported both within the public and private sectors. Many governments are paying particular attention to the energy sector, utilities such as electric companies, telecommunication companies and water suppliers, the financial sector, transportation, and health as critical underpinnings to the economy and well-being of citizens.

3) **Further scope exists for policy action to support Year 2000 readiness.** A number of countries, including *Australia, Canada, Denmark, Japan, Korea, Netherlands, Sweden, UK* and *US,* have proposed or adopted proactive policy or regulatory initiatives to support private sector readiness. These have included tax breaks and/or loan programmes for small businesses, training or other policies to encourage expansion of the Year 2000 specialist labour pool, and policies to promote information disclosure. While it is too early to judge how effective such policies will turn out to be, governments should assess such potential

solutions in their own national contexts to determine whether further policy action may be appropriate.

Lack of awareness is still a major problem

4) **Awareness and educational efforts are required to overcome incomplete understanding of the problem.** This refers not only to national government and private sector actions, but also includes efforts at the international level by such organisations as the OECD, United Nations, World Bank, European Commission and many others on the sectoral level. Several OECD countries cited difficulties answering the OECD questionnaire, particularly in central and southern Europe. In some cases, this stems from diffused responsibilities that make it difficult for the central management agencies of government to obtain an overall view of progress. It was also suggested that agencies had provided assurances that they would be ready in time, because they had recently modernised their IT systems or had relatively few to deal with. Unfortunately, even newer systems are vulnerable to Year 2000 problems, and the problem spans beyond computers. In the absence of a government-wide information campaign, smaller agencies would seem to be particularly vulnerable, due to a lack of expertise and readily available information on best practices.

5) **Regular public disclosure of government and industry assessments of readiness will help motivate action.** They can also help to build public confidence that remedial action is going forward. However, governments should also be careful to balance the need for information to assess the state of preparedness, versus the additional information-collection burdens that such reporting requirements impose.

6) **Greater focus is needed on embedded systems.** The Year 2000 problem is often misperceived as merely affecting computer systems. However, embedded systems or chips are also vulnerable to Year 2000 malfunctions, and are built into most modern electronic equipment. This includes a range of plant, equipment and appliances such as elevators, heating controls, medical equipment, traffic lights, telephone exchanges, cars, trucks, buses, aircraft, navigation equipment, water pumps, engines, automatic doors, security systems, cash tills, and many home appliances. According to the Report of the *New Zealand* Government Administration Committee, only 3 or 4 chips out of 1000 may malfunction, but this nevertheless represents a real risk.[28] Unlike with computer software, which can be reprogrammed, faulty embedded chips generally need to be replaced. Testing also poses greater challenges for embedded systems than for computers due to difficulties involved in adjusting the internal calendars within these devices. Preventing problems involves painstaking inventorying of electronic equipment and contacting of suppliers to obtain information on their Year 2000 compliance. Contingency planning should also address the possibility that vendors' assurances may be incorrect.

7) **Regional and local governments should be just as concerned.** Just as small and medium enterprises tend to lag behind larger companies in their preparations, evidence suggests that local governments often lag behind national governments in preparing for the millennium date change. In most cases, national governments have little leverage to ensure local government compliance, though often achievement of national policy involves extensive co-

28. "The Y2K Inquiry," Report of the *New Zealand* Government Administration Committee, April, 1998 (http://www.year2000.co.nz/y2kgov07.htm).

operation and exchange of data across levels of government. But countries can specifically target regional and local government awareness as part of their national campaigns.

Bringing government action to bear

8) **Y2K requires high-level managerial attention and a central strategic capacity.** Whether governments create separate co-ordinating institutions or assign this responsiblity to an existing central management agency, some central capacity for assessing and managing the problem is desirable. The interdependence of many government information systems makes this particularly important. Though devolved responsibility is well recognised as an effective management approach, an appropriate balance also should be sought between individual responsibility and the capacity to ensure an overall strategic direction and focus on vulnerable and high-priority areas. Central management agencies or specially-created bodies thus have a role to play in reviewing readiness, promoting co-operation and exchanging information, particularly regarding data exchange and necessary testing involving multiple actors.

9) **Risk assessment and contingency planning are an essential part of preparations.** Regardless of how well national governments prepare to ensure that their own operations are Year 2000 compliant, they will remain dependent on electricity, telephone systems, transportation and supply systems to continue functioning beyond the Year 2000. For these reasons, as well as the virtual impossibility of ensuring that their own systems are "Millennium bug-proof," preparation of risk assessments and contingency plans should be part of every agency's preparations. Risk assessments are necessary in their own right to determine where greatest vulnerabilities lie and to help prioritise remediation efforts. Contingency plans should take these findings into account in determining how best to continue mission-critical functions in the event of possible system failures. Given the potential for many systems to break down or malfunction well before 2000, governments take significant risks by leaving contingency planning to the end.

Greater international co-operation is essential

10) **Increased cross-border testing and international co-operation is needed.** Transport, telecommunications, international financial transactions, energy provision and many other activities depend upon cross-border interconnections that could be vulnerable to Year 2000 breakdowns. While there is at least some awareness and institutional capacity to address the problem in most OECD countries, vulnerabilities could also arise to the extent that OECD economies interact with developing countries: a study released by the World Bank in July found that only 10 percent of 120 developing nations had a government-wide Year 2000 programme. This report, including the discussion of international initiatives in sensitive sectors as described in Part I and the list of Web sites and government contacts in Annexes A and B, aims to increase awareness and encourage greater international contact and cross-border testing.

ANNEX A

National and International Governmental Web Sites on the Year 2000 Problem

These sites and an up-to-date list of other related Year 2000 sites may be found on the OECD Year 2000 links web page (http://www.oecd.org/dsti/sti/it/infosoc/news/y2klinks.htm).

Country	Name of Site	Web Site
AUSTRALIA	Autralian Gov't Office of Gov't Information Technology	http://www.ogit.gov.au/year2000/yr2000.html
	NSW Gov't Year 2000 Home page	http://www.y2k.gov.au/html/links.html
BELGIUM	Millennium Forum 2000 -Federal Gov't Forum (French)	http://www.y2000.fgov.be/index.htm
CANADA	Canadian Federal Gov't Year 2000 Information Site	http://www.info2000.gc.ca
	SOS 2000-Ministry of Industry	http://strategis.ic.gc.ca/year2000
DENMARK	Year 2000-Ministry of Research & IT	http://www.fsk.dk
EC	Year 2000 & the EURO	http://www.ispo.cec.be/y2keuro/
FRANCE	Ministere de l'Economie des Finances et d'Industrie (French)	http://www.industrie.gouv.fr/
GERMANY	Federal Ministry of Economics informs about the Development of Information Society	http://www.bmwi-info2000.de
	Das Jahr 2000 Problem-German Federal Ministry of Education, Science, Research & Tech (German/English)	http://www.iid.de/jahr2000
	Koordinieurungs-und Beratungsstelle	http://www.kbst.bund.de
HUNGARY	Informatikai Tarcakozi Bizottsag (Hungarian)	http://www.itb.hu/
ICELAND	1999/2000- Skyrr	http://www.skyrr.is/2000/
IRELAND	Y2K and the Irish Civil Service-Dept. of Finance	http://www.irlgov.ie/finance/y2k2.htm
ITALY	Autorita Per L'Informatica nella Publicca Amministrazione (Italian)	http://www.aipa.it/attivita/anno2000[11/index.asp
	Segreteria Tecnica del Ministro (Italian)	http://www.minindustria.it/Gabinetto/Seg_Tecn/ Inf2000.htm
KOREA	Y2k Focus Bulletin-Korea National Computerization Ag.	http://y2000.nca.or.kr/ENG_DIR/intro.htm
MEXICO	Proyecto Ano 2000- Secretaria de Contraloria y Desarrollo Administrativo (Spanish)	http://www.secodam.gob.mx/proy2000/
	Comision Nacional para la Conversion Informatica Ano 2000 - Politica Informatica Nacional (Spanish)	http://pdi.inegi.gob.mx/2000/
	Year 2000- Banco de Mexico (Spanish)	http://www.banxico.org.mx/public_html/t2000/ 2000.html
NETHER.	Projectbureau Millennium Overheid (Deutch)	http://www.pmo.nl
	Millennium Platform	http://www.mp2000.nl/millen/Millen.nsf/
NEW-ZLND.	Y2K Task Force- Task Force Secretariat	http://www.y2k.govt.nz/
	Government Administration Committee "Y2K Inquiry"	http://www.year2000.co.nz/y2kgov07.htm

(Continued next page)

National and International Governmental Web Sites on the Year 2000 Problem (continued)

Country	Name of Site	Web Site
NORWAY	Ar 2000-Direktoratet for Forvaltningsutvikling (Norwegian)	http://www.sol.no/statskonsult/aktuelt/historie/ar2000dp.htm
	Ar 2000 problemet i staten- Arbeids:og Adm.- Dept. (Nor.)	http://www.odin.dep.no/aad/publ/aar2000/index.html
	Aksjon 2000 (Norwegian)	http://www.aksjon2000.org
PORTUGAL	Ministry of Science & Technology (Portuguese)	http://www.missao-si.mct.pt/P2000/first.html
	Instituto de Informatica (Portuguese)	http://www.inst-informatica.pt/
	Ano em 2000 Portugal (Portuguese)	http://www.EUnet.pt/ano2000/
SPAIN	Map (Ministerio de Administraciones Publicas) 2000 (Spanish)	http://www.map.es/csi/2000.htm
	Effecto 2000 Year 2000- Grupo Parliamentario Sociolista	http://www.ctv.es/USERS/estrella/2000.htm
SWEDEN	Swedish Agency for Administrative Developments (Statskontoret)Information Systems Year 2000(Swedish)	http://www.statskontoret.se/2000/indexe.htm
	IT Commission	http://www.itkommissionen.se/
UNITED KINGDOM	Cabinet Office- Central IT Unit	http://www.open.gov.uk/citu/cituhome.htm
	UK Action 2000 -Dept. of Trade & Industry	http://www.open.gov.uk/bug2000/index2.html
	Ministry of Defense- Year 2000 Date Change	http://www.mod.uk/dgics/dcsa_web/psg_web/modyear.htm
	Millennium Bomb-UK Central Computer & Telecommunications Agency/Gov't Info Service	http://www.ccta.gov.uk/mill/cct.gui.htm
	Millennium Software Bomb-Society of IT Management	http://www.socitm.gov.uk/socy2000.htm
	Taskforce 2000	http://www.taskforce2000.co.uk/text.htm
	Y2K Status Reports	http://floor.ccta.gov.uk:8080/year2000/y2kreports.nsf
	House of Commons Science & Technology-2nd Report	http://www.parliament.the-stationery-office.co.uk/pa/cm199798/cmselect/cmsctech/342ii/st0202.htm
UNITED STATES	President's Council on Year 2000 Conversion	http://www.y2k.gov/java/index.htm
	US Federal Government Gateway for Year 2000 Info	http://www.itpolicy.gsa.gov/mks/yr2000/y2khome.htm
	CIO Gov't Research Center	http://www.cio.com/forums/government/yr2k.html

International Organisations & Associations	Web Site
Bank for International Settlements (BIS)	http://www.bis.org/ongoing/index.htm
G-8 Government-On-Line (GOL) Year 2000 International Information Directory	http://www.itpolicy.gsa.gov/mks/yr2000/g7yr2000.htm
Global 2000 Co-ordinating Group	http://www.global2k.com/
Global Millennium Foundation	http://www.globalmf.org/
International Air Transport Association (IATA)	http://144.194.16.11/y2k/Index.htm
International Chamber of Commerce (ICC)	http://www.iccwbo.org/Commissions/Financial_ services/Note_Millennium_bug_alert.htm
International Council for Information Technology in Government Administration (ICA)	http://www.ica.ogit.gov.au/
International Labour Office (ILO)	http://www.ilo.org/public/english/20gb/docs/gb271/ pfa-7-7.htm
International Organisation of Securities Commission	http://www.iosco.org/year_2000.html
International Press Telecommunications Council (IPTC)	http://www.xe.net/iptc/iptc2000.htm
International Telecommunication Union (ITU)	http://www.itu.int/y2k/
International Y2K Virtual Conference	http://www.itpolicy.gsa.gov/mks/yr2000/g7conf.htm
OECD Y2K links/ PUMA / DSTI	http://www.oecd.org/puma/gvrnance/it/index.htm http://www.oecd.org/dsti/sti/
UN Information Technology Section	http://www.un.org/members/yr2000/yr2000.htm
UNDP Info 21- The Year 2000	http://www.undp.org/undp/info21/new/n-y-disc.html
World Bank Group : Year 2000 Information Pages	http://www.worldbank.org/y2k/index.htm
World Customs Organisation (WCO)	http://www.wcoomd.org/frmpublic.htm
World Information Technology & Services Alliance (WITSA)	http://www.itaa.org/witsa.htm

ANNEX B
GOVERNMENT CONTACT POINTS AND WEB SITES

Contact for further information

Country	Contact person	Address	Tel #	Fax #	Email
AUSTRALIA	Steve Fielding, Project Manager, Year 2000 Project Office	Office of Gov't IT, P.O.Box 258, Dickson ACT 2602, Australia	61-2-6271-4836	61-2-6271-4899	steve.fielding@ogit.gov.au
AUSTRIA	Dr. Otto Hellwig, Head of the Division for the Coordination of IT in Federal Chancellery	A-1014 Wien, Ballhausplatz 2	43-1-53115-4237	43-1-53-53-650	otto.hellwig@bka.gv.at
	Mag Michael Binder, Head of the Division for Innovation & Technology Policy in the Federal ministry of Economic Affairs	A-1010 Wien, Stubenring 1	43-1-71100-5925	43-1-7142719	
BELGIUM	Ph. Bodson, Forum Millenium 2000		02/287-40-08	02/287-40-10	y.2000.fgov.be
	J.M. Mottoul, Programme Admi-2000		02/287-40-09	32-2-287-40-10	abc.ey2k@magfr.fgov.be
CANADA	Guy Mc Kenzie, Assistant Secretary	Year 2000 Project Office, Treasury Board of Canada Secretariat	613-957-8673	613-952-1516	McKenzie.Guy@t.s.sec.gc.ca
CZECH REP.	Marie Widemannova, Director of the Dept. for Public Administration Reform	Ministry of the Interior of the Czech Rep. U Obecniho domu 3, 112 20 Praha 1	4202 21101351	4202 21101349	
DENMARK	Poul Bernt Jensen	Ministry of Research and Information Technology Forskningsministeriet			PBJ@FSK.dk
	Emil Bundesen	Bredgade 43 - 1060 København K	45 33 92 9799	45 33 93 8012	ebu@FSK.dk
EC	Ms. S. Callagan, IDA Project Officer, DG III/B/6	Rue de la Loi 100, B-1049 Brussels (Mailing) Rue de la Science 15, B-1049 Brussels (Office)	322 299 0263	322 299 0286	Sandra.CALLAGAN@dg3.cec.be
FINLAND	Olavi Kongas, CIO	Ministry of Finance	358-9-160-3255	358-9-160-3299	Olavi.Kongas@vm.vn.fi
FRANCE	Gabriel de Maistre				gabriel.de-maistre@industrie.gouv.fr
GERMANY	Ernst Wilzek	Arbeitsgruppe 0 1 (KBSt), Federal Ministry of the Interior, Postfach 17 02 90, 53108 Bonn	49-228-681-2201	49-228-681-2202	Ernest.Wilzek@bmi.bund.de

(continued next page)

Country	Contact person	Address	Tel #	Fax #	Email
GREECE					
HUNGARY	Andras Szigetti, Deputy Director General	Prime Minister's Office, Coordination Office of Gov'tal Information Systems			
ICELAND	Hauker Ingibergsson		354-560-9137	354-552-8280	hauker.ingibergsson@fjr.stjr.is
	Johann Gunnarsson		354-560-9150	354-552-8280	johann.gunnarsson@fjr.stjr.is
IRELAND	Tim Duggan, CMOD	Lansdowne House, Lansdowne Rd., Dublin 4	353-1-6045065	353-1-6682182	duggant@cmod.finance.irlgov.ie
	Donal Denham	Department of Enterprise, Trade & Employment, Kildare St., Dublin 2	353-1-6614444		denhamd@entenp.irlgov.ie
ITALY	M. Busetto	Ministere de L'Industrie, Commerce et Artisanat, Cabinet du MinistreSecretariat Technique	396 47887753	396 47052244	busetto@minindustria.it
JAPON	Nobuhiro Fukuoka, First Secretary	Delegation Permanente du Japon Aupres de l'OCDE, 11 Avenue Hoche, 75008	331-5376 6100	331-4563 0544	fukuoka@deljp-oecd.fr
KOREA	Su-Wan Jang, Deputy Director, Organization Policy Division	Ministry of Gov't Administration & Home Affairs, 77-6, Segong-Ro, Jongro-Gu, Seoul, 110-760	82 2 720 4349	82 2 3703 5529	jangsuwan@hanmail.net
LUXEMBOURG	Pierre Neyens. Directeur de l'Administration du Personnel de l'Etat	B.P.516, L-2015 Bureaux: 12-14 av. Emile Reuter	478-3200	22 25 23	
MEXICO	Jose Octavio Lopez Presa,Deputy Secretary	Secretariat of Controllership & Administrative Development (SECODAM), Av. Insurgentes Sur No. 1735, 10 Piso, Ala Norte, OFNA. 1012 Col. Guadalupe Inn C.P.01020	662.28.86 ~8	662.28.89	
	Dr. Carlos M. Jarque, President of INEGI & Chairman of National Commission on Year 2000	National Inst. of Statistics, Geography & Informatics,Av. Heroe de Nacozari Num. 2301 Sur Fracc. Jardines del Parque, CP 20270 Aguascalientes, Ags.			cmjarque@pres.inegi.gob.mx

(continued next page)

Country	Contact person	Address	Tel #	Fax #	Email
NETHERL.	Drs. Ing. Peter D. Verstege, RE RA	Ministry of Interior, Projectbureau Millennium Overheid P O Box 556, 2501 CN Den Haag (Gov't Y2K Project Office) Postbus 20011, 2500 EA Den Haag	3170-376 5870	3170-376 5871	p.verstege@pmo.nl p.verstege@net.HCC.nl
NEW ZEAL.	Helen Meehan, Chief Advisor Information Managment	State Services Commission P O Box 329, Wellington	64 4 495 6622	64 4 495 6700	helen.meehan@ssc.govt.nz
	Brendan Kelly, Senior Advisor Information Management	Y2K Task Force, Dept. of the Prime Minister & Cabinet, P O Box 55, Wellington	64 4 495 6622 64 4 470 6734	64 4 495 6774 64 4 99 9027	brendan.kelly@ssc.govt.nz brendan.kelly@parliament.govt.nz
NORWAY	Hans Christian Holte	Ministry of Labor & Gov't Administration P.O.Box 8004 Dep., N-0030 OSLO	47 22 24 46 14	47 22 24 95 17	hans-christian.holte@aad.dep.telemax.no
	(General awareness/SMEs)Aksjon 2000	Mollergt. 16, P.O.Box 8044 Dep., N-0030 OSLO	47 22 24 02 66	47 22 24 02 64	aksjon2000@vinn.no
POLAND	Boleslaw Slomian, Director	Dept. of Telecommunication & IT Ministry of Interior & Administration			
PORTUGAL	Prof. Jose Dias Coelho, Chairman, Mission for the Information Society	Edificiio Green Park, Av. dos Combatentes, 43-A - 10 C, 1600 Lisboa	3511 7210918	3511 7220541	jdcoelho@missao-se.mct
	Domingos Vilia				domingos.vilia@inst-informatica.pt
SPAIN	Victor M. Isquierdo Loyola, Subdirector General de Coordinacion Informatica	Secretario del Consejo Superior de Informatica, Ministerio de Administraciones Publicas	34 91586 1899	34 91586 1920	victor.izquierdo@sgci.dgopti.map.es
SWEDEN	Lars Soderstrom	Ministry of Finance, S-10333 Stockholm	46 8 405 43 18	46 8 24 62 13	lars.soderstrom@finance.ministry.se
SWITZERL.	U. Grete	Monjiboustr. 74 3003 Bern	4131 325 9491		
TURKEY	Prof. Dr. Gurol Banger, Head of the Administration Development Dept.	Prime Ministry of Turkey	90312 4137800	90312 4138190	igb@basbakanlik.gov.tr
UK	Mandy Mayer, Head of the Year 2000 Team	Cabinet Office, Horseguards Road, London SWIP 3AL			
US	John A. Koskinen, Chair President's Council on Year 2000 Conversion	Room 115, Old Executive Office Building Washington DC 20503	202-456-7171	202-456-7172	Koskinen_J@A1.eop.gov

ANNEX C

QUESTIONS TO NATIONAL GOVERNMENTS REGARDING THE "YEAR 2000 PROBLEM"

A. ASSESSMENT OF THE PROBLEM

		Yes	*No*
1)	Has the government wholly or partially estimated national, **economy-wide impacts of** addressing the problem? *If yes,* what are the expected economic impacts in 1999 and 2000? Please provide Web site references, excerpts or **copies of studies on the impacts** of the year 2000 problem in your country -- real or potential -- that may have particularly influenced the government's policy to address the problem.	❑	❑
2)	Has the national government estimated its **budget costs** of addressing the problem? *If yes,* how much in 1998? in 1999?	❑	❑
3)	Is **auditing and testing** of government systems to determine whether they are "Year 2000-compliant" already under way? *If yes,* how far has auditing and testing progressed and what are the most recent results regarding government systems' compliance to handle the Year 2000 date change?	❑	❑
4)	Has an overall **risk assessment** of the problem in the government sector been done? *If yes,* what were its conclusions?	❑	❑

B. GOVERNMENT POLICY FOR ADDRESSING THE PROBLEM

5)	Does the policy establish priorities for addressing **internal operations** (e.g. identification of most vulnerable and mission-critical functions or programmes in government)? *If yes,* what are they?	❑	❑
6)	Does the policy address electronic **data exchange with non-government computers**? *If yes,* how?	❑	❑
7)	Does the policy establish priorities for addressing specific **sectors of the economy** (e.g. communications, emergency services, energy, finance, transport, utilities); *If yes,* what are these priority areas?	❑	❑
8)	Does the policy define the government's role in promoting or ensuring **action in the private sector?** *If yes,* what is the government's role (e.g., raising awareness, imposing requirements, providing subsidies, co-ordinating action, etc.).	❑	❑

C. INSTITUTIONS FOR CO-ORDINATING AND PROMOTING ACTION

		Yes	No
9)	Is there a designated organisation or individual responsible for promoting co-ordinated action on this issue at the **national** level? *If yes*, please identify and indicate how co-ordination is being handled (e.g. within national government, across levels of government, priority sectors, or across economy).	❑	❑
10)	Is there a designated organisation or individual responsible for promoting co-ordinated action on this issue at an **international** level? *If yes*, please identify and indicate how co-ordination is being handled (e.g., participation in international organisations, conferences, cross-border data exchange, etc.).	❑	❑
11)	Is there an institution(s) responsible for promoting **awareness** of the problem? *If yes*, what actions are being undertaken to promote awareness?	❑	❑

D. GOVERNMENT IMPLEMENTATION

12)	Has a system of **reporting on preparations and compliance** of systems been established? *If yes*, how frequently are results reported? What are the most recently available results?	❑	❑
13)	Have **contingency plans** been developed for alternative courses of action in the event of system failure? *If yes***,** please describe.	❑	❑
14)	Have **budgeting policies** specifically addressing Y2K preparations been established? *If yes*, please describe (e.g., provision of extra funding, expedited resource allocation, diversion of funding from other purposes, withholding of funding until certain thresholds are met).	❑	❑
15)	Have **regulations** been established specifically addressing Y2K preparations? *If yes*, please describe and/or attach.	❑	❑
16)	Are specific **rewards or sanctions** being used to promote Y2K compliance? *If yes*, please describe.	❑	❑

Please provide the name and address of a contact person, phone number, fax, and e-mail address, for any follow-up that may be necessary.

ANNEX D
INTERNATIONAL RECOMMENDATIONS FOR GOVERNMENT ACTION

Joint Year 2000 Council

1. The Joint Year 2000 Council, an international task force focusing particularly on world financial markets, issued a press release in July, 1998 recommending strongly "that all countries develop a national strategy with respect to the Year 2000 problem. . . National governments can play an important role in promoting broad-based awareness at the most senior level of the private and public sector of the potential disruptive effects of the millennium date change; in ensuring that appropriate action is taken by all major institutions in the economy, including utilities; and in co-ordinating action taken by different industries in both the public and private sector, both domestically and internationally."

2. The press release notes that experience in a number of countries which have developed and implemented concerted national Year 2000 strategies suggests that the following tasks could usefully be assigned to a national government co-ordinating body:

- Improving awareness of the complexity of the Year 2000 challenges in both the private and the public sectors;
- Co-operating with relevant private sector organisations to ensure that proper action is taken in all sectors of the economy to achieve Year 2000 readiness by all users of information technology, both large and small;
- Paying particular attention to readiness efforts of major utility providers such as electricity companies, telecommunication companies and water suppliers;
- Establishing target dates for completing key phases of Year 2000 programmes appropriate for the industry and market;
- Evaluating the available human and financial resources to address the Year 2000 problem in key industries;
- Ensuring proper action by various government agencies to minimise possible disruptions relating to the millennium date change;
- Assessing the possible cross-border aspect of the Year 2000 problem and assisting in the international co-ordination of national strategies;
- Developing and implementing a communications strategy to increase public confidence as the millennium date change approaches;
- Assisting in the co-ordination of contingency planning in both the private and public sector.

3. The Joint Year 2000 Council is co-sponsored by the Basle Committee on Banking Supervision, the Committee on Payment and Settlement Systems, the International Association of Insurance Supervisors, and the International Organisation of Securities Commissions. The Council's Secretariat is provided by the Bank for International Settlements, which also brings together information and contact points on a range of international initiatives on its Web site (http://www.bis.org).

World Information Technology and Services Alliance

4. WITSA specifically recommends that governments and international organisations adopt the following five-point "Year 2000 Survival Plan":

1) Individually and collectively, governments and international organisations should announce their commitment to solving the year 2000 challenge, thereby calling attention to its importance. Progress should also be publicly reported at regular intervals.

2) Each national government should immediately allocate sufficient financial and human resources to fix the most essential year 2000 problems for its own government, and take appropriate actions to [create] incentives [for] sub-national governments to do the same. In so doing, they may need to devote additional funds so that existing IT programs of national importance are completed.

3) Adjust government practices to ensure that future procurement of computer and communications systems recognise the requirement to process dates though the year 2000.

4) Each national government should take appropriate action make the non-governmental sector aware of the need to re-assess priorities to address the year 20000 computer problem. Business should be especially alerted to their systems which interact with other business and which are therefore reliant on each other to address the issue in a timely manner.

5) Identify systems of national importance and ensure there are plans for then to be fixed in time. These may include:

- Communications - Telecommunications and data networks
- Emergency Services - Police, Ambulance and Fire
- Energy - Generation and supply
- Finance - Banking and trading
- Food Supply - Shipping storage and distribution
- Manufacturing - Supply chains and automated process control system
- National security - Defence and intelligence services
- Public health - Hospital equipment and systems
- Small and medium sized enterprises - Supply chains, manufacture and distribution
- Government Exchequer - Tax collection, customs and excise, and welfare payments
- Transport - Air, trains, traffic systems, mass transit systems
- Utilities - Water supply and waste management

International Council for Information Technology in Government Administration

5. This international network of government officials responsible for dealing with government information technology systems developed a set of recommendations in August, 1997, based on the consensus of representatives from the following countries: Australia, Canada, Denmark, Finland, Germany, Ireland, Israel, Netherlands, Norway, Portugal, Slovak Republic, Sweden, Switzerland, United States, United Kingdom.

- **The need for action is urgent.** Many Information Technology (IT) managers predict that their systems will fail before 2000 because they include processes for short term forecasting. December 31 1999 is not the target deadline it is the absolute and final time by which all systems must be corrected, tested and implemented.

- **Top management must take charge** of, and assume responsibility for, their organisation's Year 2000 programme. The breadth of issues dictates that it will be insufficient to attempt to drive the required process from a middle management perspective. Senior management holds the key to setting the agenda and the correct priorities for their organisation.

- **Government must take a lead role** in addressing the Year 2000 date change issues and maintain an overall government responsibility. The implications are far reaching and may affect all levels of society.

- **In the public sector the prime objective is to ensure that the sector's ability to continue to provide services is not threatened.** Procedures for monitoring Year 2000 activities inside the public sector are required. Methods for retaining key staff should be developed. Budget implications and resource allocation procedures should be considered. The testing phase should not be underestimated. Public sector buying power should be used to ensure co-operation and involvement from vendors. Year 2000 compliance certificates should be agreed with suppliers.

- In regard to public utilities, governments must ensure awareness and require appropriate activity. Government must also take the lead in promoting awareness within the private sector.

- **The subject of embedded systems is a major cause of concern** because of the general lack of information and this aspect requires special attention.

- **Year 2000 problems do not stop at the border of a country.** Co-ordination of standards for data interchange is required. No organisation, committee, league, or entity has taken responsibility for a world-wide view of problems and solutions. International Relations and a well co-ordinated approach is therefore needed. The relationship of the problems in advanced countries to less advanced countries has not been defined. The awareness issues should become the responsibility of the advanced countries.

- The risk of introducing new major IT intensive projects, such as the European Economic and Monetary Union (EMU) related enhancements, in parallel with Y2000 conversion, can create conflicting demands and this should be considered.

- Many public sector bodies have said that they intend to achieve Year 2000 compliance through the use of existing resources. This means that new IT applications and services

cannot be developed and introduced if all existing resources are dedicated to the Year 2000 problem. The key point here is that it is widely recognised that IT resources are fully allocated to the Year 2000 problem, and that skill shortages are likely to occur.

6. ICA officials reconvened at the end of June 1998 (with additional participation from Hungary, Malta, the OECD and European Commission), and reaffirmed the value of their previous recommendations. They found that much progress had been made since their initial workshop, and that participating governments appeared to be taking a common approach in many areas: information campaigns, including distribution of booklets and other information on the subject, information services on the internet, and close follow-up on public sector initiatives. However, the group underlined several "continuing and growing concerns," including the need for critical and realistic review of plans; contingency planning; effective testing; review of embedded systems; supply chains; cross-border issues; and transparent information to promote awareness, action, accountability, and public confidence.

ANNEX E
THE OECD INTERNAL YEAR 2000 INITIATIVE

1. The OECD launched its formal work on the Year 2000 problem in early 1996 with a preliminary analysis of the scope and impact on the Organisation. The analysis confirmed that there were a number of areas which required corrective action -- whether in hardware, software and data. A number of mission-critical computer systems and related databases were identified, mainly operating on mainframe computers, which were not Y2K compliant, including the three major in-house applications: the Main Economic Indicators (MEI) database system, the Financial Management Information System (FIMS), and Payroll/Pension.

2. In view of the potentially serious impact that non-compliant Y2K systems could have on the work of the Organisation, important decisions were made in 1996, which placed highest priority on resolving Y2K problems on mission-critical systems and applications. To this end:

- The Board of Directors for Computer and Communications Technology Strategies (CCTS) established an inter-Directorate Steering Group to oversee internal Y2K activities;

- A formal project management approach and a five-phased Y2K methodology was adopted, identifying the list of actions and plans for the:

    1. Awareness Phase
    2. Assessment Phase
    3. Renovation Phase
    4. Validation Phase
    5. Implementation Phase

- A Year 2000 Project team was set up to address all centrally-managed computer and communications systems.

- On an international level, the Statistical Policy Group assumed responsibility for co-ordinating actions with external data providers and users on matters relating to OECD information. The Y2K Project Team maintains contacts and shares information and experiences with other international organisations and independent advisory organisations on best practice approaches to resolve internal Y2K issues.

- The OECD Operations Service assumed responsibility for reviewing and ensuring compliance of electronic devices, including a review of their embedded systems.

- An action plan was established to address non-centrally managed systems of client Directorates and Services, which is briefly described below.

– Contingency plans will be prepared this autumn with top priority systems specifically identified, such as Publications, analytical/statistical applications and payroll.

3. As of July 1998, the OECD had identified 644 systems and applications - including hardware, operating systems and related software, application systems, and desktop applications - 45 per cent of which are Y2K compliant or have been discontinued, 49 per cent are partially compliant, and 6 per cent are not Y2K compliant. Results are updated continuously.

THE OECD INTERNAL YEAR 2000 ACTION PLAN

Year 2000 Awareness Programme

– Information notes to programme managers;

– Presentation(s) to the CCTS Board of Directors;

– Presentation in meetings of Directors and information systems correspondents;

– Cinema sessions to increase awareness of OECD staff;

– Articles posted on the Intranet and the Contact Newsletter;

– Application-specific meetings, where required.

Inter-Directorate Steering Group

– Establishment of an inter-Directorate Steering Group to take stock of potential problem areas, share common experiences, and develop early action schedules. The Group will in particular refine the present action plan and update it as required.

Year 2000 Technical Team

4. The Information Technology and Network (ITN) Service has established a special Year 2000 technical team to oversee and co-ordinate all technical aspects of this important project. The role of this team includes:

– Verify hardware and software compliance with manufacturers for all centrally operated computing and communications systems.

– In liaison with clients in Directorates and Services, identify external data sources which need to be assessed for Year 2000 compliance

– Advise Directorates/Services on the standard methodology to resolve Year 2000 problems

– Establish, early next year, a "Year 2000 Centre" which will be equipped with computers with dates pre-set to allow users to test their programmes and databases for Year 2000 compliance (during the transition from 1999 to 2000, as well as after January 1, 2000).

5. The Y2K project is scheduled for completion by mid 1999.

REFERENCES

Airlines International Magazine (1998), Vol. 4, Issue 3, May-June.

Bank of England (1998), "Financial Sector Preparations for the Year 2000".

Bank of Montreal (1998), Special Report: "Some Thoughts on the Year 2000 Problem and the Economy", April, http://www.bmo.com/economic/special/y2k.htm

Bureau of National Affairs (BNA) (1998), *Year 2000 Law Report*, May, July issues.

Business Week (1998), "Zap ! How the Year 2000 Bug will Hurt the Economy", February.

Canada Task Force 2000 (1998*a*), *A Call for Action*, February. http://strategis.ic.gc.ca/SSI/yk/eng.pdf

Canada Task Force 2000 (1998*b*), *A Call for Action: The Eleventh Hour*, July. http://strategis.ic.gc.ca/SSI/yk/neweng.pdf

Cap Gemini (1998), Press Information, PR 1053, April.

Center for Strategic and International Issues (CSIS) (1998), proceedings from the conference "The Y2K Crisis: A Global Ticking Time Bomb?", June. http://www.csis.org/html/y2ktran.htm

Coopers & Lybrand (1997), *Year 2000 Survey Results*, November.

European Commission (1998), Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, The Year 2000 Computer Problem, COM(1998)102, Brussels.

European Commission - DG III (1998), *Draft Report from Second Workshop on National and Sectoral Initiatives on the Year 2000 Computer Problem*, Brussels, March.

European Information Technology Observatory (EITO) (1998), *EITO 98*, Frankfurt/M.

Federal Deposit Insurance Corporation (FDIC) (1998), "FDIC Announces Results of Year 2000 On-site Reviews", PR-37-98, June. http://www.fdic.gov/publish/newprs/1998/pr9837.html

Gartner Group (1998), World-wide and Industry Readiness.

Goldman Sachs (1998), US Economics Analyst, Issue No. 98/22, June.

Hancock Rothert & Bunshoft, *Legal Update on the Millennium Bug Liability*, various issues. http://www.2000law.com/html/newsletters.html

Health and Safety Executive (HSE) (1997), *Safety and the Year 2000*, HSE Books.

Health and Safety Executive (HSE) (1998), *Health and Safety and the Year 2000 Problem*, May. http://www.open.gov.uk/hse/year2000.pdf

IBM (1998), *The Year 2000 and 2-Digit Dates: A Guide for Planning and Implementation*, Document Number GC28-1251-08, February. http://ppdbooks.pok.ibm.com:80/cgi-bin/bookmgr/bookmgr.cmd/BOOKS/y2kpaper/CONTENTS

Info2000 Canada (1998), *Braiter/Westcott Report on Year 2000 Readiness*, February, http://www.info2000.gc.ca/Communications/GovtRpts/BraiterRptE.html

ING Barings (1998), *Defusing the Time Bomb: A Millennium Survey*, Global and Emerging Markets Research, May.

Institution of Electrical Engineers (IEE) (1997), *The Millennium Problem in Embedded Systems*, November. http://www.iee.org/2000risk/guide/httoc.htm

International Air Transport Association (IATA) (1998), Press release: "IATA expands Year 2000 Effort with IATA Project 2000", January. http://www.iata.org/y2k/project2000.htm

International Data Corp. (IDC) (1997), "Status of the Year 2000 Problem around the Globe", November.

International Telecommunication Union (ITU) (1998), Press Release ITU/98-21, May.

Japan Information Service Industry Association (JISA) (1997), "Results of the Survey with a Questionnaire to Users on the Year-2000 Problem (summary)", September. http://www.jisa.or.jp/statistics/y2k-97-e.html

Joint Year 2000 Council (1998), *Fact Sheet*, May. http://www.bis.org/ongoing/y2kintro.htm

J.P. Morgan Securities Inc. (1996), "The Year 2000 Problem: Ready or Not, Here It Comes", Equity Research, July.

Knolmayer, Gerhard (1998), "Sixteen fundamental theses on the state of solving the Year 2000-Problem in Switzerland, Institut für Wirtschaftinformatik (IWI), University of Bern, April. http://www.ie.iwi.unibe.ch/zobis/survey1997_media1998.htm

Knolmayer, Gerhard (1997), "How (and what) is Europe doing on Y2K ?", Paper presented at the 4th International Conference on Year 2000 Computing, Association of Information Technology Professionals, SIG-Mainframe, New York, http://www.ie.iwi.unibe.ch/zobis/jahr2000/europe.pdf

Lloyd's Register (1998), "For when the bug bites", 100A1, Issue 1, January. http://www.lr.org/news/a1/100A1198.pdf

Merrill Lynch (1998), *Y2K: Implications for Investors*, Special Report, June.

Moody's Investors Service (1998), *The Bugs and the Banks: European Banks face the Twin Challenge of the Year 2000 and the Euro Conversion*, May.

Morgan Stanley (1997), "Y2K Watch: Digital Plague Oozes Across Planet", US Investment Research, March.

New Zealand Government Administration Committee (1998), *The Y2K Inquiry: Inquiry into the Year 2000 Date Coding Problem*, April

OECD (1998), *OECD Economic Outlook 63*, June.

Oxford Economic Forecasting (1998), "Global Economic Effects of Year 2000", Press Notice, July.

PA Consulting Group (1998), *Defusing the Millennium Bomb: the Embedded Software Threat - A Survey of UK Awareness and Readiness.*

PA Consulting Group (1997), *Defusing the Millennium Bomb: an International Survey of Awareness and Readiness.*

PaineWebber (1998), *Banks & Y2K*, June.

Pirkle & Associates (1998), http://www.pirkle-websites.com/solcomp.htm

Reserve Bank of Australia (RBA) and Australian Prudential Regulation Authority (APRA) (1998), *Year 2000 Preparations in the Australian Banking and Financial System*, July. http://www.rba.gov.au/new/y2k.pdf

Software Productivity Research (SPR) (1997), *The Global Economic Impact of the Year 2000 Software Problem*, v.5.2, January. ftp://ftp.spr.com/articles/y2k52.pdf

Statistics Canada (1998*a*), *The Preparedness of Canadian Business for the Year 2000 Computer Problem*, Small Business and Special Surveys Division, February, http://www.statcan.ca/english/freepub/61F0057MIE/0019861F0057MIE.pdf

Statistics Canada (1998*b*), The Daily, July 6. http:///www.statcan.ca/Daily/English/980706/d980706.htm

Swiss Reinsurance Company (Swiss Re) (1997), *The millennium muddle*, Zurich. http://www.swissre.com/download/public/millen-e.pdf

UK Parliament, House of Commons, Science & Technology Committee (1998), *Second Report: The Year 2000 - Computer Compliance*, April. http://www.parliament.the-stationery-office.co.uk/pa/cm199798/cmselect/cmsctech/342ii/st0202.htm

UK Treasury (1998), *Economic Impact of the Millenium Bug*, World Economic Issues.

US Federal Reserve Board (1998), Testimony of Governor Edward W. Kelley Jr. before the Committee on Commerce, Science, and Transportation, US Senate, April 28. http://www.bog.frb.fed.us/BOARDDOCS/TESTIMONY/19980428.htm

US General Accounting Office (GAO) (1998), *Year 2000 Computing Crisis: Potential for Widespread Disruption calls for Strong Leadership and Partnerships*, GAO/AIMD-98-85, April

US Office of Management and Budget (OMB) (1998), Progress on Year 2000 Conversion: 5th Quarterly Report, May.

US Securities and Exchange Commission (SEC) (1998*a*), Staff Legal Bulletin No.5 (CF/IM), January. http://www.sec.gov/rules/othern/slbcf5.htm

US Securities and Exchange Commission (SEC) (1998*b*), Interpretation: Disclosure of Year 2000 Issues and Consquences by Public Companies, Investment Advisers, Investment Companies, and Municipal Securities Issuers. http://www.sec.gov/rules/concept/33-7558.htm

World Bank (1998), Press Release: *infoDev Initiative to Address the "Millennium Bug"*, April. http://www.worldbank.org/infodev/y2knews.htm

Yardeni, Edward (1998), "Year 2000 Recession ?" v. 7.2, July. http://www.yardeni.com/y2kbook.htm

Yardeni, Edward (1998), The Y2K Reporter, Deutsche Bank Research, various issues, http://www.yardeni.com/y2kreporter.html

Congressional testimonies:

Canadian Parliament, House of Commons, Standing Committee on Industry:

- Report 6: "The Year 2000 Problem - Where is Canada Now ?" (May 1998).

- Transcripts of Hearings on IT and Preparedness for the Year 2000: 28 May 1998, 21 April 1998 (afternoon) and 21 April 1998 (morning), 24 March 1998, 19 March 1998, 17 March 1998, 12 March 1998, 9 March 1998, 19 February 1998, 17 February 1998, 10 February 1998.

US House of Representatives Hearings:

- Committee on Ways and Means, Subcommittee on Oversight: The Year 2000 Computer Problem and Telecommunication Systems (16 June 1998), Hearing on the Year 2000 Computer Problem (7 May 1998);

- Science Committee, Subcommittee on Technology: Millennium Short Circuit: The Y2K Effect on Energy Utilities (14 May 1998), Government-wide Year 2000 Issues and the Department of Treasury (18 March 1998), FAA at Risk: Y2K Impact on the Air Traffic Control System (4 February 1998), The Global Dimensions of the Millennium Bug (4 November 1997);

- Committee on Government Reform and Oversight, Subcommittee on Government Management, Information and Technology: Oversight of the Federal Government's Year 2000 Efforts (18 March 1998),

US Senate Hearings:

- Banking, Housing and Urban Affairs Committee: Disclosure of Year-2000 Readiness (10 June 1998); Office of Thrift Supervision's Year-2000 Preparedness (18 March 1998); The Implications of the Year 2000 Computer Problem (17 February 1998); FDIC's Year-2000 Preparedness (10 February 1998); Mandating Year-2000 Disclosure by Publicly Traded Companies (4 November 1997); Year 2000 Liability and Disclosure (22 October 1997); Financial Institutions Regulators' Management of the Year-2000 Computer Problem (30 July 1997); Financial Institutions and the Year 2000 Problem (10 July 1997);

- Commerce, Science and Transportation Committee: Year 2000 Computer Problem (28 April 1998)

ACRONYMS

ACI: Airports Council International.

APRA: Australian Prudential Regulation Authority.

ASX: Australian Stock Exchange.

ATA: Air Transportation Association.

ATAC: Air Transport Association of Canada.

BIS: Bank for International Settlements.

BT: British Telecommunications.

CAA: Civil Aviation Authority.

CAPP: Canadian Association of Petroleum Producers.

CGA: Canadian Gas Association.

CN: Canadian National Railway.

CSSIN: Conseil Supérieur de la Sûreté et de l'Information Nucléaires.

DOE: Department of Energy.

EITO: European Information Technology Observatory.

EMU: Economic and Monetary Union.

EOW: End-of-week.

EPRI: Electric Power Research Institute.

ETIS: European Telecommunications Informatics Service.

FAA: Federal Aviation Administration.

FCC: Federal Communications Commission.

FDA: Food and Drug Administration.

FDIC: Federal Deposit Insurance Corporation.

FERC: Federal Energy Regulatory Commission.

GAO: General Accounting Office.

GPS: Global Positioning System.

HSE: Health and Safety Executive.

IATA: International Air Transport Association.

ICA: International Council for Information Technology in Government Administration.

ICAO: International Civil Aviation Organisation.

ICC: International Chamber of Commerce.

IDC: International Data Corporation.

IEA: International Energy Agency.

IEE: Institution of Electrical Engineers.

IETF: Internet Engineering Task Force.

infoDev: Information for Development

IT: Information technology.

ITU: International Telecommunication Union.

JISA: Japanese Information Service Industry Association.

JSDA: Japanese Securities Dealers Association.

NEA: Nuclear Energy Agency.

NEI: Nuclear Energy Institute.

NERC: North American Electric Reliability Council.

NRC: Nuclear Regulatory Commission.

NZSE: New Zealand Stock Exchange.

OCC: Office of the Comptroller of the Currency.

OEF: Oxford Economic Forecasting.

OMB: Office of Management and Budget.

PSTN: Public Switched Telephone Networks.

RBA: Reserve Bank of Australia.

S&P: Standard & Poor's.

SBA: Small Business Administration.

SEC: Securities and Exchange Commission.

SIA: Securities Industry Association.

SPR: Software Productivity Research.

UKAEA: United Kingdom Atomic Energy Authority.

WCO: World Customs Organisation.

WITSA: World Information Technology and Services Alliance.

Y2K: Year 2000.