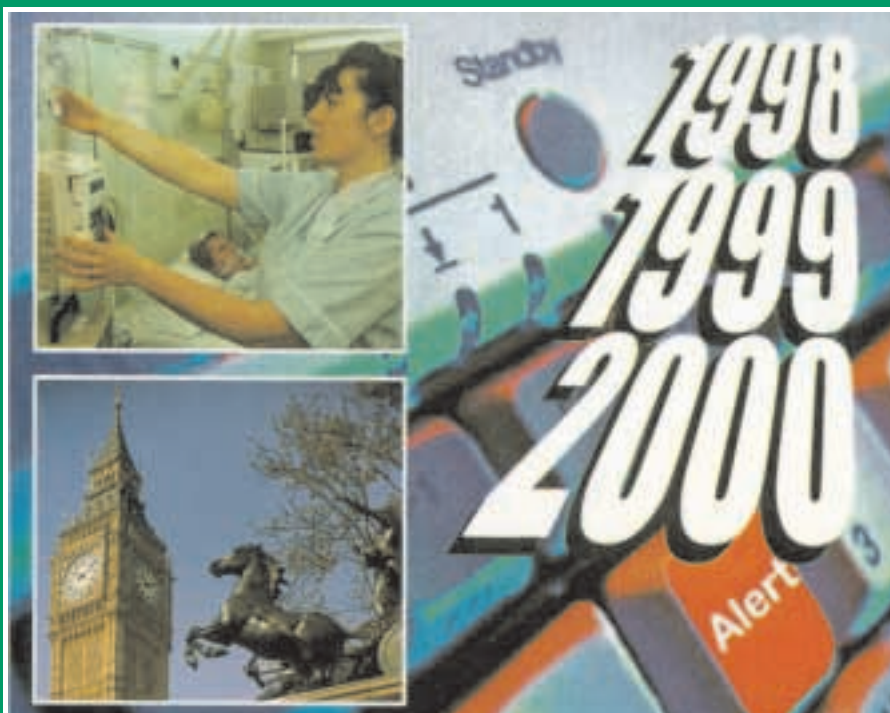


# Managing the Millennium Threat II



This report has been prepared under Section 6 of the National Audit Act 1983 for presentation to the House of Commons in accordance with Section 9 of the Act.

*John Bourn*  
Comptroller and Auditor General

National Audit Office  
8 May 1998

The Comptroller and Auditor General is the head of the National Audit Office employing some 750 staff. He, and the National Audit Office, are totally independent of Government. He certifies the accounts of all Government departments and a wide range of other public sector bodies; and he has statutory authority to report to Parliament on the economy, efficiency and effectiveness with which departments and other bodies have used their resources.

For further information about the National Audit Office please contact:

National Audit Office  
Press Office  
157-197 Buckingham Palace Road  
Victoria  
London  
SW1W 9SP

Tel: 0171-798 7400

email: [nao@gtnet.gov.uk](mailto:nao@gtnet.gov.uk)

Web site address: <http://www.open.gov.uk/nao/home.htm>

# Contents

<b>Executive summary</b>	<b>1</b>
<hr/>	
<b>Part 1: Progress by central government</b>	<b>10</b>
Summary	10
Monitoring government departments and agencies	11
Timescales	13
Coverage of embedded systems	14
Availability of skills and resources	15
Coverage of third party links	16
Adequacy of business continuity planning	17
Costs	17
Other centrally funded public sector bodies	19
Monitoring progress	20
Wider action	21
Conclusions	22
Recommendations	24
<hr/>	
<b>Part 2: Year 2000 compliance in the NHS in England</b>	<b>25</b>
Summary	25
Introduction	26
Risks to the NHS	26
IT systems	26
Responsibility for achieving year 2000 compliance	28
Action taken	29
Progress	32
Conclusions	41
Recommendations	43
<hr/>	
<b>Part 3: Year 2000 compliance in the Department of Social Security</b>	<b>45</b>
Summary	45
Introduction	45
Risks to DSS	46
Responsibility for achieving year 2000 compliance	47

Action taken	48
Progress	52
Conclusions	54
Recommendation	55

**Appendices**

1. Potentially critical dates which some systems may fail to manage correctly	56
2. Co-ordinating government responses to the year 2000	57
3. Departments and Agencies making returns to the Central Information Technology Unit	59

# Executive summary

## Managing the millennium threat

**1** In our first report on Managing the Millennium Threat last May (HC 3, Session 1997-98), we warned about the potential consequences of the inability of many computers and other items of electronic equipment to handle the date change on 1 January 2000. This second report updates progress across the central government sector, and describes in more detail how the Department of Social Security and the National Health Service are tackling the problem.

**2** Other relevant reports are a forthcoming management paper by the Audit Commission which assesses year 2000 preparations in a sample of local government and NHS organisations, and the Second Report of the Select Committee on Science and Technology: "The Year 2000 – Computer Compliance".

### The Threat

**3** To save memory space, many computer programmers have in the past adopted the practice of referring to years by their last two digits rather than by all four, 98 rather than 1998; and as a consequence some computers now cannot tell the year 2000 and the year 1900 apart. This could mean that some computers and electronic equipment will produce meaningless information or fail completely. There are a number of dates which may trigger these problems. See Appendix 1 for details.

**4** From an initial view that the millennium threat was mainly an IT problem, many organisations have realised that it will have a much wider impact in other areas including:

- electronic equipment such as telephones, security systems, medical equipment and lifts, which are not traditionally thought of as computers or IT systems, may contain microprocessors which are affected by the millennium date change.
- most organisations depend on customers or suppliers of services, materials, water, gas and electricity. Even if its own internal systems and equipment are year 2000 compliant, an organisation may still be unable to continue functioning if others in the supply chain fail.

- the demand for skilled staff on year 2000 projects and similar projects, such as the introduction of the single European currency, is rising rapidly and research by Cap Gemini, a major IT consultancy company has suggested that demand for staff would outstrip supply early in 1998.

**5** As the Prime Minister said in his speech to the Action 2000/Midland Bank Conference on 30 March 1998 the situation is serious, since there are few, if any, areas of modern life that are not touched by IT and the year 2000 issue is ticking away inside many computers, mainframes and electronic systems all over the world. The Prime Minister announced a series of measures to help raise awareness in the private sector; to deal with the specific problems in the public sector; and to ensure that the national and international infrastructure is as ready as it can be. As regards the wider public sector, he concluded that estimates which put the total public cost at up to £3 billion were reasonable – although there was the possibility that they would increase.

**6** The three examples opposite illustrate the scale and potential consequences of failure to tackle the Year 2000 issue, and the need for effective contingency plans in case some systems fail.

**7** Witnesses to the Select Committee on Science and Technology of the House of Commons also drew attention to wide and serious potential consequences if the threat was not addressed, including:

- serious and prolonged damage to the whole of the rail industry;
- serious consequences in terms of failure to continue to supply oil and gas;
- malfunctions in safety-critical or essential operations, such as air traffic control; road or rail signalling; medical equipment; the water and waste control industry.

---

**Case 1    The United States of America: Federal Aviation Administration Systems**

---

The General Accounting Office reported that the Federal Aviation Administration's progress in making its systems ready for the year 2000 has been too slow, and that at its current pace it will not make it in time. The potential consequences included degraded safety, grounded or delayed flights, increased airline costs, and customer inconvenience.



---

**Case 2    Shell UK: Gas and Oil Supply**

---

Shell UK, giving evidence to the Science and Technology Committee, described some of the problems they faced in a typical offshore oil platform which uses up to 10,000 microprocessors, half of which are critical to the business. If Shell had taken no action there would be no environmental or safety risks, but the supply of gas and oil would be suspended. Shell UK are spending an estimated £40 million to ensure all their critical systems are compliant.



---

**Case 3    Medical equipment in the National Health Service with embedded chips: Infusion Pumps**

---

The British Standards Institute Year 2000 group has identified a problem with intravenous infusion pumps which give very accurate drug dosages to patients over a period of time. If these pumps are not recalibrated every six months they shut down as a safety device. At the year 2000, if the clock in the embedded computer chip is not year 2000 compliant, the equipment will assume it was last recalibrated 100 years ago and stop functioning. This could have serious consequences for patients.



## **Key responsibilities for stimulating action in the United Kingdom**

**8** In the United Kingdom, the Department of Trade and Industry have taken steps to alert British industry to the problem and to encourage industry to put in place programmes to ensure year 2000 compliance, initially through the work of Taskforce 2000. In September 1997 the President of the Board of Trade announced the creation of Action 2000 to stimulate and support the efforts of British industry in tackling this problem, through national publicity, an advice hotline for small and medium sized businesses and encouraging large companies to support action up and down their supply chains.

**9** For central government departments and agencies, each department is responsible for its own compliance programme. Individual departments also lead on areas of the wider public sector and the private sector for which they have sponsoring interests. At the centre in the Office of Public Service, the Central Information Technology Unit (CITU) and the Central Computer and Telecommunications Agency (CCTA) have a monitoring, advisory and co-ordination role, and CITU provides policy advice to ministers. The CITU monitoring role has recently been extended to cover the full public sector and a risk assessment across essential services in the national infrastructure. CITU and CCTA have raised awareness of the problem, issued guidance to departments and agencies, set a timescale for action and are monitoring progress. The Office of Public Service's timetable for action has been:

### **(a) audit of information systems**

all departments should have completed an audit of their information systems for year 2000 compliance by January 1997;

### **(b) action plans**

all departments should have prepared a prioritised, costed, and timed programme of action by October 1997;

### **(c) testing of modified systems**

all departments should have tested all modified systems by January 1999 except for financial systems where testing should have been completed after the end of the financial year, ie April 1999.



The responsibility for these actions rests with individual departments and agencies.

### **What progress have Central Government Departments and Agencies made?**

**10** Our examination of the progress reports made to the Office of Public Service suggest that not all departments and agencies have yet identified the full extent of the millennium threat, fully assessed the risks involved and prioritised work needed to manage these tasks. Under the headings set out in paragraph 9 above, our findings are:

#### **(a) audit of information systems**

We stated in our first report that most departments and agencies were at the stage of auditing their systems in January 1997. All departments and agencies have by now completed their stocktake of information systems, although the scope of their programmes has gone beyond purely IT systems.

#### **(b) action plans**

Most departments have plans with target dates for completion by January 1999. We noted the following weaknesses in these plans, however:

- The variable content of the plans and in some cases lack of detail, make it difficult to assess the realism of the targets. There are indications that some departments are already planning completion dates after January 1999 and that others already foresee slippage. Many departments are setting a range of target dates, differentiating between business-critical and non-critical systems.
- No information is held centrally on the readiness of bodies in the wider public sector, for example the 1,100 NDPBs or local authorities. In March 1998, the remit of the Ministerial subgroup on the Millennium Date Change was widened to cover the whole of the public sector as well as government departments.

- Half of the original plans made no mention of work on equipment with embedded microprocessors, although by March 1998 all but a few bodies had plans covering non-IT systems. And departments have been slow to address the risks of failure in their supply chain.

### **(c) testing of modified systems**

It is too soon to say whether departments will meet the dates of January and April 1999 for testing modified systems. Overall departments and agencies claim that they have the necessary skilled resources available in house or from existing suppliers of contracted out services, but there is a risk that as more detailed work is done, revealing the need for additional skilled staff, sufficient staff will not be available, or costs will rise as departments and agencies find they have to pay premium rates. Already the Ministry of Defence have signalled their concerns about emerging staff shortages.

We are concerned that over half of the bodies examined have not yet developed contingency plans for what they will do if their modified systems do not work. The Prime Minister recognised that this is a serious issue when he said on 30 March, “Every organisation must put in place contingency plans in case failures occur in its own systems or in other people’s.”

**11** By March 1998 the overall cost estimates to address the millennium threat for central government departments and agencies had risen by 6 per cent to £393 million. Some plans are still incomplete in scope or cost and we consider there is a risk of the overall cost estimates rising again.

### **What progress has the NHS made?**

**12** In May 1996 the NHS Executive set up a small project team to assess the impact of the millennium threat, and to alert the NHS to the problem by organising seminars and issuing information packs which the NHS found useful and relevant. But in 1997, in common with many organisations as more information became available, they took a stronger line establishing targets for action, clear accountability for results, senior management leadership, and closer monitoring of the situation. The framework for managing the remedial programme is now in place but its size and complexity are such that very tight control will now be required at all levels to ensure success.

**13** The timetable set by the NHS Executive allows 9 months from completing detailed plans and budgets in March 1998 to all critical systems being ready and fully tested, or detailed plans made for coping without these systems or equipment that cannot be repaired or replaced in time, by 31 December 1998. Our survey in October 1997 (conducted before the NHS had had time to take account of the NHS Executive timetable) showed that one fifth of NHS Trusts and Health Authorities thought they would need right up to the end of 1999 to ensure all their IT systems were year 2000 compliant, and 10 per cent of NHS Trusts were not confident that they would achieve this. Fifteen per cent of NHS Trusts were not confident that all their clinical equipment would continue functioning normally in the year 2000. Where systems or equipment cannot be repaired or replaced in time, the NHS is required to have detailed plans in place for coping without those systems or equipment.

**14** Research by one leading computer services company has shown that it will take organisations with more than 500 employees on average two and a half years to resolve the year 2000 problem. If this average applies to the NHS, Trusts and Health Authorities will need to work significantly faster than other large organisations to meet the NHS Executive deadline of having all critical systems ready and fully tested or detailed contingency plans in place, by 31 December 1998. From our survey, it is clear that NHS Trusts have concerns about being able to meet the timescale and we conclude that some parts of the NHS remain at risk of failing to achieve year 2000 compliance by 31 December 1998, the date set by the NHS Executive.

**15** The limited information available at present on the state of readiness in General Practice suggests that as a body GPs are likely to have difficulty in achieving compliance. Although individual GP practices should not present particularly complex problems and the major suppliers have year 2000 compliance programmes in hand, the sheer numbers involved, the range of systems in use and the difficulty of ensuring that action is taken by every GP, present a challenge to all concerned, including the NHS Executive. Almost all Health Authorities considered that there was not a good level of awareness among GPs of year 2000 issues, and almost one third did not have confidence that GP systems would be year 2000 compliant in time.

**16** Responses to our survey suggest that the cost to the NHS of year 2000 programmes may be in the order of £170 million, and for GP systems at least another £60 million, giving a total estimate of £230 million for the whole NHS though these figures need to be treated with caution. This is at the lower end of the range of costs for similar sized organisations which, if applied to the NHS, would suggest costs between £200 million and £850 million. NHS organisations have

been told by the NHS Executive to plan to meet the cost of their year 2000 compliance programme from within existing budgets and the NHS Confederation have expressed concern about the possible diversion of funds away from other capital projects.

**17** Inadequate resourcing increases the risk of failure, and the single largest area of concern raised in response to our survey was about the difficulties they anticipated in providing adequate resources. The NHS Executive have warned that the cost of skilled assistance on year 2000 projects is increasing and availability is reducing. This will put further pressure on year 2000 project budgets, to the extent that external assistance is required.

### **What progress has the Department of Social Security made?**

**18** The Department's approach to project management complies with best practice recommended by CCTA.

**19** On the business-critical mainframe systems, the Department has a clear plan to achieve compliance by August 1998 except for the Job Seekers Allowance payment system where the target is October 1998. At the end of 1997 they were on target and providing they continue to manage the programme carefully, they are on schedule to achieve compliance by their target dates.

### **What needs to happen now?**

**20** In the light of these findings, our main recommendations are:

All public bodies should:

- ensure that their plans fully cover the risks posed by failures in embedded systems and links with other organisations as well as in IT systems;
- take account of risk factors such as shortage of skilled staff, and prioritise action according to the risk and impact of failure on critical business functions;
- draw up contingency plans to ensure the continuity of critical business functions;

- ensure that they have robust financial information systems in place which enable them to control and account for public funds.

The Office of Public Service should:

- specify the information it requires in progress reports to enable a clear assessment to be made that the targets set by departments and agencies are achievable;
- assure itself that departments and agencies have robust business continuity plans in place;
- consider the immediate need for periodic surveys of the wider public sector to inform Parliament of the state of readiness of the public sector as a whole.

The NHS Executive should:

- continue to monitor progress very closely, taking immediate action if necessary, to ensure that all Health Authorities and NHS Trusts successfully complete all elements of the project;
- consider the need for further selective direct intervention in those cases where progress reports from NHS Trusts and Health Authorities indicate a risk of failing to achieve year 2000 compliance, or inadequate contingency plans to cope with failures in systems or equipment;
- with Health Authorities, increase efforts to inform GPs of the full consequences of year 2000 problems and through stringent monitoring assure themselves that GP services will not be disrupted by the year 2000;
- regularly review the need for further investment of resources in year 2000 projects in the light of progress reports from NHS Trusts and Health Authorities.

The Department of Social Security should:

- continue their well structured approach to achieving year 2000 compliance, monitoring progress closely and taking immediate remedial action if timetables slip.

# Part 1: Progress by central government

## Summary

**1.1** This part looks at progress made within government, based on the plans which have been produced by departments and agencies at the end of October 1997 and February 1998.

**1.2** Our overall conclusion is that although most departments and agencies met the requirement to produce costed plans by the end of October 1997, many of these were incomplete at that time and a few remained so by March 1998. The plans were highly variable in content making it difficult to assess whether departments and agencies are likely to deal with the threat successfully, and at what cost.

**1.3** The plans show that most departments and agencies have a target date for completion of January 1999, but there are some warning signs that target dates are beginning to slip. The Office of Public Service observes that many departments are setting a range of target dates, differentiating between business-critical and non-critical systems.

**1.4** The plans available suggest an overall cost for departments and agencies of just over £393 million. But some reports did not include complete assessments of costs. Costs rose by 6 per cent between November and March and experience from the private sector suggests that costs may rise again as plans are refined.

**1.5** There is evidence from the plans and progress reports to suggest that departments and agencies are vulnerable to risks of failure which have not been fully assessed and that in many cases robust contingency plans have yet to be developed.

**1.6** There is no central information on the state of readiness in the wider public sector including smaller government funded bodies, such as the 1,100 non-departmental public bodies which account for £22 billion of expenditure. Yet, research by PA Consulting highlights that small to medium sized enterprises are at relatively higher risk because they often lack the awareness, skills and resources necessary.

## Monitoring government departments and agencies

**1.7** Although the principal responsibility for ensuring that systems are year 2000 compliant rests with individual departments, the Central Information Technology Unit (CITU) within the Office of Public Service have responsibility for ensuring that the government's response to the year 2000 date change is co-ordinated and coherent, that adequate support and advice is given to departments and that progress is monitored. Appendix 2 outlines the role of CITU prior to 30 March 1998 and the changes that have been made since. The Office of Public Service has set out a programme of action to ensure that central government's response to the millennium threat is co-ordinated and coherent. The main milestones:

- ✓ all departments should complete an audit of their information systems for year 2000 compliance by January 1997;
- ✓ all departments should finalise a prioritised, costed, timed programme of action by October 1997;
- ✓ all departments should have tested modified systems by January 1999 except for financial systems where testing should have been completed after the end of the financial year, ie April 1999.

**1.8** All departments and agencies were set a deadline of producing costed plans by the end of October 1997. Sixty two plans were published in November 1997, covering 31 government departments and their agencies - see Appendix 3 for details of bodies identified. These plans were of variable content and format. They ranged from complete project plans with interim reports, to single page letters setting out some current activities. The level of detail included was variable and it was difficult to compare and assess progress from them. For example not all plans:

- included complete costs;
- covered all areas of activity, for example, embedded systems;
- included overall targets and milestones against which progress could be measured;
- included a statement of risks that were foreseen and the way in which they were being managed.

**1.9** Subsequently the Chancellor of the Duchy of Lancaster wrote to bodies in November 1997, asking for additional information about:

- finding and retaining skills and resources;
- the scope and progress of plans covering embedded systems; and
- contingency plans.

**1.10** In March 1998 the Central Computer and Telecommunications Agency (CCTA) carried out the first quarterly survey as promised by the Chancellor in his November statement. The plans, additional information and results of the March 1998 survey have also been placed in the Library and published on the Internet at Web site address: <http://www.open.gov.uk/citu/y2000.htm>

**1.11** The Chancellor of the Duchy of Lancaster made a written statement to the House on the basis of his analysis of the plans. On the same day he wrote to Ministers reminding them of the need:

- to obtain assurances from suppliers of non-IT goods and services; and
- for compliance projects to cover embedded systems and external dependencies.

He subsequently wrote to Ministers advising them to use their internal auditors to provide assurance on their department's compliance processes.

**1.12** The Northern Ireland Office is conducting an entirely separate monitoring exercise on Government departments in Northern Ireland. The summarised results are also published on the Internet at the same address as in 1.10.

**1.13** In the following paragraphs we highlight the conclusions drawn from our examination of these reports, in terms of:

- ability to meet the timescales set centrally;
- coverage of embedded systems;
- availability of skilled staff;



- coverage of links to third parties;
- adequacy of contingency planning;
- costs.

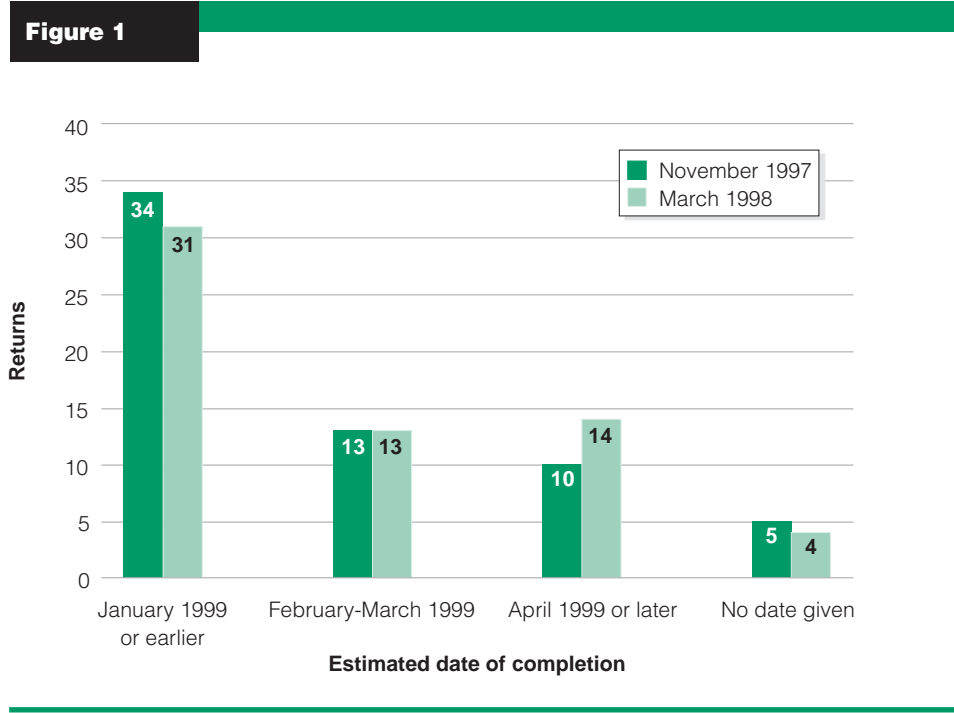
## Timescales

**1.14** The Office of Public Service set a target date of January 1999 for completion of testing of all modified systems except financial systems where the target date is April 1999. These dates were chosen to allow modified systems a year in which to settle down and some time for unforeseen problems to be corrected. The date is to some extent arbitrary as some systems, particularly IT ones, may fail before 2000. Nevertheless other commentators warn against running compliance plans “up to the wire” and leaving no margin for error. For example, the Office of the Auditor General, Canada, in its report of October 1997 recommended that Canadian government departments “allow a complete fiscal cycle to address unanticipated issues” and “target implementation for April 1998”.

**1.15** The March 1998 survey showed that overall 4 departments and 7 agencies had slipped completion targets back since November 1997. 44 per cent of returns expected testing to be completed after January 1999, of which 23 per cent have dates of April 1999 or later. One department stated that although January 1999 remained their target they already foresaw slippage beyond that date. The Office of Public Service observes that many departments are differentiating between business-critical and non-critical systems, and also identifying systems that may fail earlier than others, and setting a range of target dates accordingly. Changes in completion dates need to be judged in this context.

**1.16** Figure 1 compares the estimated dates for completion of compliance work declared by 62 plans in November 1997 with the dates declared in March 1998. This shows that although the majority of respondents had and still have a target date of January 1999 or earlier, the percentage has declined over five months.

Target dates for completion reported in November 1997 and March 1998



## Coverage of embedded systems

**1.17** All of the plans published in November 1997 covered progress made towards tackling the problem as it affected IT systems, and showed that in many cases the projects were led and dominated by IT departments. In almost half of the plans no mention was made of progress towards identifying or fixing the threats posed to embedded systems.

**1.18** However the December responses to the Chancellor’s letter showed that all bodies had plans to cover embedded systems, though in many bodies it was clear that this work was running behind the work on IT systems. This may be reasonable if failure in embedded systems presents a lesser threat to the operation of the business than the failure of IT systems. However there was no evidence in the responses indicating that this judgement was based on a systematic assessment of risks. Action 2000 has warned that the consequences of failure of embedded systems could range from trivial through disruption to dangerous and that businesses would be negligent if they assumed that any breakdowns would only be trivial.

**1.19** The March 1998 survey showed that by then most bodies had costed plans covering embedded systems but 6 returns still showed them outstanding, although all expected to complete the audit phase quickly. For example, the Department of Health was at that time unable to estimate costs for both their Voice and Video, and Embedded Systems work. The Chancellor again wrote to colleagues on the day of his March statement reminding them that project scopes needed to include embedded systems.

**1.20** A good example of the way that the scope of year 2000 programmes has changed is given in the preface to the March return from an Agency:

“The year 2000 programme has developed significantly since original plans were requested in October and has moved from being IT system based to an all encompassing business focussed programme looking at estates, contracts, suppliers, legal, regions, small systems and end user computing, contingency (IT systems and Local Offices) as well as main IT systems.”

**1.21** The Highways Agency (of Department of Environment, Transport and Regions) March return included work on building systems, the trunk road highway network infrastructure and type approval of traffic control equipment. Earlier returns only covered IT. As a result, their estimated costs have risen threefold from £4.3 million to £14.3 million.

## **Availability of skills and resources**

**1.22** Many commentators have warned that the fixed deadline of the millennium threat means that competition for skills and resources will drive the prices up and that in extreme cases resources will be unavailable.

**1.23** A very large majority of departments and agencies however are confident that they have the necessary resources and skills to complete their plans. Their returns in both December 1997 and March 1998 show that 90 per cent are happy to rely on their in-house resources, those of their existing suppliers of contracted-out services or a combination of the two.

**1.24** A few plans identified staff as a risk factor - specifically the retention of key staff throughout the project. Similarly a few plans identified finance as a constraint. In these cases the plans outlined the consequences and action to compensate where possible. For example Companies House and the Office of National Statistics outlined their policies to encourage the recruitment and retention of skilled staff. The Home Office say that cost constraints may stop them working on making low priority systems compliant.

**1.25** There has been little change in this picture between the responses in December to the Chancellor's letter in November and the March progress reports, with one exception. The Ministry of Defence reported in March that "In house resources are limited and, whilst these will be used in so far as they are available, many areas will be looking to consultancy support to get the work completed. There are early signs of shortages of extra-mural resources". It is not clear yet what the impact of this will be on costs or the ability of the Ministry to meet its timescales.

## Coverage of third party links

**1.26** As well as having a direct impact on the business capability of an organisation, the Millennium Threat will also affect that organisation's business partners, suppliers, customers and agents which in turn may have a consequential impact back on the organisation. Although the impact of business failures in third party partners is difficult for an organisation to manage, government bodies must assess and manage the risks arising, including developing robust business continuity plans (see section 1.29-1.31).

**1.27** Of the 62 original plans, 42 made no explicit reference to business partners or to the ways in which departments intended to manage the risks that they posed. The March 1998 survey asked departments about:

- their progress in checking the compliance of interfaces with other organisations; and
- the assurances they have received from their suppliers of IT and other equipment.

**1.28** The responses to the March 1998 survey were more positive. Nearly 80 per cent of returns identified interfaces and 36 per cent showed the bodies had audited the compliance of their interface with other organisations. Most bodies had at least contacted their suppliers, however the level of assurance they were

getting was varied. For example the Radiocommunications Agency (DTI) found that suppliers were generally helpful but included many caveats. The experience of CCTA was that their results were variable and they considered that further testing was needed. The Chancellor wrote in March 1998 to colleagues reminding them of the importance of this aspect of compliance.

## Adequacy of business continuity planning

**1.29** Bodies need to bring their business continuity plans up to date to deal with the impact of failure of not just their own systems but of third party systems on their business operations. Some plans included evidence that risks had been assessed, work prioritised and contingency plans put in place. Less than 20 per cent of returns in March 1998 indicated that bodies considered that they had adequate continuity plans covering their business critical systems, most of the rest needed to update existing plans or create new ones.

**1.30** A small proportion of bodies consider such plans as unnecessary, and several bodies dismissed the need for continuity plans on the grounds that they are confident their own compliance programmes will be successful.

**1.31** The British-North American Committee, made up of 87 academics and senior business people from Britain, the USA and Canada, warned in January 1998 of the potentially serious impact of the Millennium Threat on public services and advised that “contingency plans, inside and outside government, are needed to deal with the failures that may occur despite the most diligent effort.” The Office of Public Service comments that they have sought further detailed information on departments’ business continuity planning, in recognition that the matter needed to be taken very seriously by departments.

## Costs

**1.32** Based on plans submitted, the Chancellor of the Duchy of Lancaster reported to the House of Commons on 27 November 1997 on how departments and agencies were tackling the problem. He announced that the total estimated cost then was just over £370 million. More than half the total estimated cost was accounted for by a single department - the Ministry of Defence has estimated that its costs will be “in the region of £200 million”, to cover all its remedial work to computer systems, operational (weapons) systems and command and control systems. The reports did not cover bodies in Northern Ireland nor organisations in

the wider public sector such as local authorities or the National Health Service. The Prime Minister, in a speech to the Action 2000/Midland Bank Conference on 30 March 1998 said that estimates which put the total public sector cost at up to £3 billion are reasonable.

**1.33** Originally eight plans from government departments and agencies excluded estimated costs. A further eighteen reports included costs that were incomplete in some way. These included reports which:

- estimated staff time but had not expressed that in cash terms;
- excluded the costs of compliance work in agencies;
- included costs for only early stages of their compliance programme;
- excluded costs for work on embedded systems and/or third party links.

**1.34** These findings are similar to those in a recent report by PA Consulting Group, [Defusing the Millennium Bomb - An International Survey of Awareness and Readiness, published in November 1997], based on their Millennium Surveys. This report was based on data from 1,000 public and private sector organisations in fifteen countries, and 12 per cent of responses were from central government, government agencies and local authorities. The report showed that at that stage 29 per cent of respondents were unable to estimate the cost of their programmes and pointed to an increased risk of project failure when costs are inadequately assessed.

**1.35** The experience of many organisations, public and private alike, shows that costs tend to rise as the problems are investigated. Cap Gemini's survey estimates that the cost to UK organisations of fixing the year 2000 problem has risen from £23 billion in October 1997 to £31.8 billion in February 1998, a rise of 38 per cent.

**1.36** Within central government between November 1997 and March 1998, 13 reports showed reported increased costs totalling £20.6 million though some bodies still cannot produce complete costs, particularly for non-IT systems. (There was a small downward movement where four bodies reported reductions of just under £1 million.) The increases were due in part to improved budgeting but mainly due to increased scope. The revised total estimated cost given by the Chancellor in his statement on progress on 3 March 1998 was £393 million, a rise of 6 per cent.

## Other centrally funded public sector bodies

**1.37** The returns published since November 1997 do not cover the 1,100 or so non-departmental public bodies (NDPBs), accounting for expenditure of some £22.4 billion of which £18.5 billion is funded by government. To date, therefore, there has been no central assessment of the extent to which these bodies are addressing the millennium threat although each sponsoring department has been asked by the Chancellor to monitor progress. This concern is heightened by research by PA Consulting Group which suggests that smaller organisations are behind in understanding the likely impact of the problem.

**1.38** Also outside the scope of the returns are:

- Public Corporations e.g. BBC, Bank of England;
- Nationalised Industries e.g. Post Office, Civil Aviation Authority;
- NHS bodies (see Part 2);
- Local Public Spending Bodies;
- Northern Ireland Departments, although the NIO report a budget for compliance of just under £9 million.

On 30 March the Prime Minister announced the establishment of a new Year 2000 Team in CITU, which among other activities, will co-ordinate and monitor across the whole public sector (see Appendix 2).

## Monitoring progress

**1.39** The Chancellor in his November 1997 statement said that departmental plans needed continuous monitoring and that further reports would be requested and published quarterly, starting in Spring 1998. This process has started and he made a further report to Parliament on 3 March 1998. For the future, CITU plans to:

- issue, collate and publish quarterly returns, the last one being expected in March 2000;
- to produce general guidance, seminars and working parties through CCTA;
- continue to support the role of the Chancellor in informing Parliament and the public about progress;
- provide constructive feedback to departments in particular cases.

**1.40** The Office of Public Service have developed a more detailed and structured quarterly progress review questionnaire, sent out at Easter 1998. This seeks additional information on:

- predicted and actual costs by quarter;
- progress towards completion for critical, non-critical, embedded and telecommunications systems;
- staffing and resourcing;
- departmental risk assessment, impact analysis and business continuity planning in respect of IT systems and supply of goods, services and information.

The questionnaire is accompanied by a feedback note from CCTA to departments covering general lessons and issues raised by previous review.



## Wider action

**1.41** The Prime Minister has established a Ministerial Group on the Millennium Date Change (MISC4), chaired by the President of the Board of Trade, to drive action across the whole of the public and private sectors, while continuing to give priority to preparing the national infrastructure for the millennium date change. A Sub-group chaired by the Chancellor of the Duchy of Lancaster is charged with driving action across central government departments, agencies and the wider public sector to prevent damage from failure of electronic systems related to the year 2000 date change.

**1.42** The Department of Trade and Industry have also taken steps to alert British industry to the threats and encourage them to put in place programmes to ensure year 2000 compliance. Through the work of Taskforce 2000 the government has raised awareness, and in September 1997 the President of the Board of Trade announced the creation of Action 2000 to stimulate and support the efforts of British industry in tackling the issue. Action 2000 will work in partnership with Government and the private sector to reduce the impact of the millennium date change on the UK economy to an acceptable risk.

**1.43** Action 2000 has set itself the following objectives in order to achieve its mission:

- To raise awareness across the small and medium sized enterprises community and provide the necessary support to allow correction of the problem.
- To work with large businesses to ensure that supply chains are fully addressed and to develop best practice.
- To develop a strategy to address the technical aspects of the Millennium Bug.
- To work with Government to ensure the maintenance of public services and to contribute to a contingency plan.
- To contribute to the international dimension in support of the Government.
- To implement a programme to increase public confidence as the millennium date approaches.

Action 2000 has set up a Hotline for public access to advice and support. This is supplemented by a world wide web site. The National Computing Centre has been contracted to operate a “Bugnet” whereby business may exchange experience and good practice. Of particular concern to Action 2000 at this time is the state of readiness of small and medium sized enterprises, the impact that these will have on the supply chain, and the effects of embedded software on all businesses.

## Conclusions

### Will departments and agencies be ready in time?

**1.44** Most of the plans have a target date for completion of January 1999. The highly variable content of the plans, however, and in some cases lack of detail, make it difficult to assess how realistic these targets are. And there are warning indications in the progress reports that some departments are already planning completion dates after January 1999 and that others already anticipate slippage against that date. The Office of Public Service observes that many departments are differentiating between business-critical and non-critical systems, and also identifying systems that may fail earlier than others, and setting a range of target dates accordingly. Changes in completion dates need to be judged in this context.

**1.45** No information is held centrally on the readiness of bodies in the wider public sector, for example the 1,100 NDPBs or local authorities.

### Is the extent of the millennium threat fully realised?

**1.46** The returns submitted to CITU in March 1998 do not give confidence that all Departments and agencies have yet identified the full extent of the millennium threat, have fully assessed the risks and have prioritised work to resolve the problem. The Office of Public Service observes that the best remedial programmes generally result in some re-scoping and re-prioritisation: the best approach therefore is one of regular and open monitoring and updating of plans.

**1.47** Half of the original plans made no mention of work on equipment with embedded systems. By March 1998 all but a few bodies had plans covering non-IT systems. For some departments the additional work was very significant.

**1.48** Departments have been slow to address the risks of millennium failure in their supply chain.

### **Do departments and agencies have the necessary skilled staff?**

**1.49** Overall departments and agencies appear confident that they have the necessary skilled resources available in-house or from existing suppliers of contracted-out services. But there is a risk that as more detailed work is done, sufficient staff will not be available, or costs will rise as they have to pay premium rates.

### **Are business continuity plans in place?**

**1.50** The evidence from the plans and progress reports in March 1998 suggest that departments and agencies are still vulnerable to risks of failure which have not been fully assessed. Many bodies do not have contingency plans in place, and a small proportion of bodies consider such plans as unnecessary.

### **Do departments and agencies know how much it will cost?**

**1.51** Half of the reports published in November 1997 included incomplete cost estimates and eight reports had no cost estimates at all. By March 1998 some cost estimates were still incomplete and the overall budget had risen. The evidence from the private sector suggests that costs could rise as departments and agencies refine their plans and begin their remedial work. These factors suggest that the March 1998 estimate of £393 million for central government departments and agencies could be an underestimate.

### **Is progress being monitored effectively?**

**1.52** The Office of Public Service is committed to monitoring progress and reporting to Parliament, but there was still variation in the format of the plans published in March 1998, and the content of the plans was highly variable. This makes systematic monitoring and comparison very difficult and time consuming.

**1.53** A clear common format for the content of progress plans would enable the Office of Public Service to add more value by identifying departments and agencies most at risk of failure and feed back general lessons and experience to all departments and agencies. It would also enable the Office of Public Service to come to a more informed view about the overall risk the year 2000 problem poses to government business and identify more easily priorities for further action.

### **Will the wider public sector be ready?**

**1.54** There is as yet no central information on the state of readiness in the wider public sector, although failures in this area could impact on central government departments and on the wider economy. Research in the private sector suggests that smaller bodies may be more vulnerable to failure.

## **Recommendations**

**1.55** In the light of these findings, we recommend:

- The Office of Public Service should specify the information it requires in the progress reports to enable a clear assessment to be made that the targets set by departments and agencies are achievable.
- The Office of Public Service should assure itself that departments and agencies have robust business continuity plans in place specifically to deal with the millennium threat.
- The Office of Public Service should consider the immediate need for periodic surveys of the wider public sector to inform Parliament of the state of readiness of the public sector as a whole.

## Part 2: Year 2000 compliance in the NHS in England

### Summary

**2.1** This part examines the risks faced by the NHS in England, the action taken by the NHS to ensure that it can continue functioning normally in the year 2000, and progress so far. Action taken by the Department of Health to ensure their internal systems are year 2000 compliant has not been examined, but their progress report has been included in Part 1.

**2.2** Our overall findings are that, initially, the NHS Executive set up a small project team to assess the impact of the millennium threat. In common with many organisations, as more information became available, there was a growing realisation of the seriousness of the problem and more recently they have put in place the framework of a well managed project with responsibility for achieving year 2000 compliance resting with the Chief Executives of Health Authorities and NHS Trusts and each GP practice. Health Authorities and Trusts have been set timescales for action which are challenging, with shorter timescales than the average for similar sized organisations if they are to be effectively compliant by 31 December 1998 (the date required by the NHS Executive). Formal, regular monitoring of progress has only recently been established and the limited information available on the state of readiness in General Practice suggests that, as a body, GPs are likely to have difficulties in achieving compliance.

**2.3** If those NHS Trusts and Health Authorities who were able to give us estimates in response to our survey in October 1997 are typical, we estimate the cost of achieving year 2000 compliance is £170 million for all NHS Trusts and Health Authorities with at least a further £60 million for GPs. This is at the lower end of the range of costs for other organisations of similar size, and could rise when detailed costed plans are finalised.

**2.4** Based on the results of our survey and on research findings in other public and private sector organisations, our assessment at this stage of the project is that, although considerable effort is being expended on the issue by all parts of the NHS and a well considered project framework is now in place, parts of the NHS risk not being ready for the millennium equipped with compliant systems or able to manage the consequences of non-compliance by December 1998. To further reduce the risk of failure the NHS Executive will need to continue to monitor

progress in NHS Trusts and Health Authorities very closely, increase efforts to inform GPs of the full consequences of year 2000 problems and assure themselves that GP services will not be disrupted, and in the light of progress regularly review the need for further resources and consider the case for further selective direct intervention where NHS Trusts or Health Authorities are at risk of failing to achieve compliance or having adequate contingency plans in place.

## Introduction

**2.5** The Department of Health, through the NHS Executive, is responsible in England for the provision of GP, hospital and community healthcare services. 100 Health Authorities and around 3,500 GP Fundholding Practices purchase healthcare services from over 400 NHS Trusts. In addition there are almost 29,000 GPs who are self-employed practitioners with contracts for service with the Health Authorities.

**2.6** Some 800,000 people currently work in the NHS providing 10.5 million episodes of hospital care at a cost of £33.5 billion. The NHS currently spends around £200 million each year on IT, and over £100 million buying medical and surgical equipment.

## Risks to the NHS

**2.7** The NHS Executive have advised all NHS Trusts and Health Authorities that there could be serious disruption to the NHS in the year 2000 unless urgent pre-emptive action is taken. They have stated that it is impossible to predict the seriousness of malfunctions but in extreme circumstances failure or malfunction of equipment could even put patients lives at risk. The Chief Executive of the NHS has described the year 2000 problem as “the highest non-clinical priority in the NHS.”

## IT systems

**2.8** Much of the NHS relies heavily on IT systems for many of the services which patients require, including managing appointments, waiting lists and keeping track of patient records. Many of the more sophisticated support services, for example in laboratories, use computers extensively. Between 8,000 and 9,500 GP practices are computerised with an estimated 29 million patient records in England dependent to some extent on IT systems in GP practices. Some 8-10 per cent of GP practices keep all their patient records on computer, and GP computer systems generate around 285 million prescriptions each year. The financial management systems which enable the NHS to pay its staff, purchase and pay for

essential supplies and maintain financial control all depend heavily on computers. The NHS is moving towards greater reliance on electronic transfer of financial and clinical information, including making patient test results and records electronically available when they are needed. As the links between systems grow the risks also increase of a failure in one system affecting other systems.

**2.9** Failure in any of these systems could mean clinical information being delayed or lost, administrative disruption for patients, doctors and nurses, and staff and suppliers left without payment. The consequences of failure will vary, with the potential effects on acute hospital trusts being greater than on smaller community trusts. Some systems need to be able to handle dates beyond 31 December 1999 already, for example, for appointments and recall arrangements for screening services.

### **Electronic equipment**

**2.10** The use of electronic equipment systems controlling sophisticated equipment is also widespread in the NHS. Many of the more sophisticated laboratory, x-ray and other diagnostic and treatment services rely extensively on electronic equipment with embedded computer chips, and failure of these systems could have serious consequences for patients. Failure of non-medical equipment could also seriously affect patients, for example failure of air-conditioning equipment could close operating theatres. Many devices and installations depend on the correct operation of several other items of equipment. There is thus the possibility of multiple simultaneous failures.

### **Links with other organisations**

**2.11** Although most of the computer links are internal to the NHS, there are some electronic links with external bodies such as banks for paying salaries, and in some cases with suppliers to order and pay for goods. Even where there are no electronic links, the NHS relies on the continuing functioning of many other organisations, including all the public utilities and suppliers of goods and services, such as important clinical supplies.

**2.12** In common with most organisations, an interruption in the normal supply of utilities, goods and services could seriously disrupt the normal working of many NHS organisations.

## Responsibility for achieving year 2000 compliance

**2.13** The responsibility for ensuring that IT systems and other equipment continue to work in year 2000 rests with the Chief Executives of the 100 individual Health Authorities and 400 NHS Trusts. In addition each GP practice has responsibility for ensuring that their system continues to work in the year 2000, though Health Authorities are responsible for monitoring progress and providing advice and assistance.

**2.14** Year 2000 problems affect many aspects of the work of the NHS and lead responsibility for providing advice and guidance on year 2000 issues to Health Authorities, NHS Trusts and General Practitioners has been assigned to four main specialist areas:

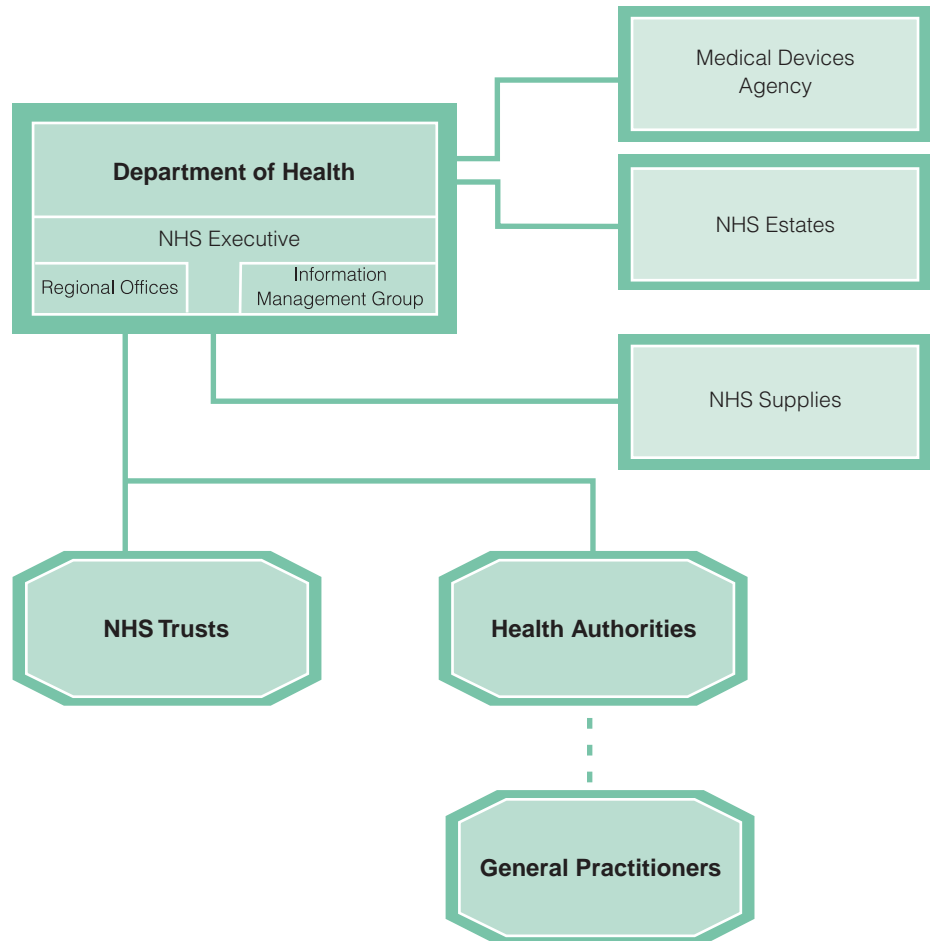
- The Information Management Group of the NHS Executive gives advice and guidance to the NHS on all IT related issues.
- The NHS Supplies Authority provides advice and purchasing services for a wide range of goods and services.
- The NHS Estates Agency provides specialist advice and consultancy on estate matters, including equipment.
- The Medical Devices Agency is responsible for taking all reasonable steps to safeguard the interests of patients and users by ensuring that medical devices and equipment meet appropriate standards of safety, quality and performance.

**2.15** Figure 2 shows the various organisations in the NHS who are responsible for advising and ensuring IT systems and equipment continue to function normally in the year 2000.



Organisations in the English NHS

**Figure 2**



**Action taken**

**Initial action 1995-1996**

**2.16** In 1995 the Information Management Group of the NHS Executive sought to raise awareness by encouraging the health computing press to publish material about the year 2000. The Information Management Group set up a small project in May 1996 to assess what action the NHS needed to take to address potential year 2000 problems. The NHS Executive first wrote directly to Chief Executives of Health Authorities and NHS Trusts on the potential problems of the year 2000 date change in September 1996. Chief Executives were asked to ensure that all systems

using computers were reviewed and that management and technical arrangements were put in place to correct systems where necessary. Health Authorities were also asked to make sure that GPs in their area were aware of the problem and dealing with it.

**2.17** The Information Management Group of the NHS Executive sent out information packs to Health Authorities, NHS Trusts and GPs giving advice on how to set up a Year 2000 Project. They also organised a series of seminars to raise awareness and set up a helpline for queries on the year 2000 date change issue. Almost all Health Authorities and NHS Trusts who responded to our survey found the guidance they had received from the NHS Executive useful and relevant.

**2.18** The main focus at this stage was on IT systems and non-medical equipment which used embedded computer chips. At that time, medical equipment was outside the scope of the NHS Executive's project and was dealt with separately by the Medical Devices Agency. Chief Executives were told that the Medical Devices Agency, an executive agency of the Department of Health, was examining the issue and had come to a preliminary conclusion that medical devices might show some year 2000 problems, but these were unlikely to be serious and very unlikely to be life-threatening.

**2.19** The primary responsibility for taking remedial action was with the 500 or so Chief Executives, supported mainly by the Information Management Group of the NHS Executive. A small project team was set up to co-ordinate action in the NHS initially concerning IT services only. A specific timescale was not set for action, though Chief Executives were told that they should know where they stood before the end of 1996.

### **Subsequent action 1997-1998**

**2.20** In April 1997 the Information Management Group of the NHS asked Chief Executives of NHS Trusts and Health Authorities to confirm that they had made arrangements to deal with the millennium threat. While 40 per cent of NHS organisations reported on the arrangements they had set up, it was considered that further commitment on the part of Chief Executives was required.

**2.21** In October 1997 the NHS Executive instructed Chief Executives of NHS Trusts and Health Authorities to take personal responsibility for ensuring patient services were not compromised by this problem. Around the same time, the NHS Executive established a national steering group and a national year 2000 task force, based on an existing experienced IT team, to provide a speciality national resource, and give assistance to the NHS. Two exemplar projects were also funded by the NHS Executive to gain and disseminate experience on year 2000 issues.

**2.22** A challenging timescale was set out by the NHS Executive, which required:

- all initial plans to be completed by 30 November 1997;
- detailed project plans, including how and when contingency plans were to be developed, detailed inventory and budgets estimates completed by 31 March 1998;
- all critical systems ready and fully tested or detailed plans made for coping without those systems or equipment that cannot be repaired or replaced in time, by 31 December 1998.

**2.23** From 1 January 1998 the Regional Offices of the NHS Executive assumed responsibility for monitoring progress against these deadlines as an integral part of their performance management responsibilities.

**2.24** NHS organisations were instructed by the NHS Executive in October 1997 to draw up inventories of electronic equipment, prioritise equipment whose failure would have serious consequences, contact suppliers for advice, take corrective action if necessary and draw up contingency plans for equipment failure. The Medical Devices Agency also issued a bulletin to all medical equipment manufacturers advising them to assess all their products, identify any affected by year 2000 problems and make this information available to users with an indication of the appropriate remedial action by the beginning of 1998. They also emphasised the need to prioritise action stating that “the resources do not exist, nationally or globally, to investigate every item of hardware and software in use throughout industry and commerce, let alone to put right all those that have not been correctly designed for the year 2000.”

**2.25** The Medical Devices Agency, however, advised users of medical equipment not to test commercial products but to await advice from suppliers. If no advice had been received from suppliers by early 1998, users were to approach the suppliers. If no satisfactory reply had been received within two months, the Medical Devices Agency was to be informed.

**2.26** The NHS Executive also advised that the many unknown elements meant that not all malfunctions could be predicted and therefore extensive precautionary plans needed to be implemented, with disaster recovery plans in some circumstances. The NHS also has to prepare for the possibility of an increase in demand for its services, building on existing plans for dealing with major incidents, if people are harmed by year 2000 related failures in other organisations' systems. Malfunctions affecting patients, the public or staff could result in legal action so all actions taken in dealing with the year 2000 problems were to be scrupulously recorded to demonstrate the steps which had been taken to avoid adverse events.

**2.27** The NHS Executive told Health Authorities and NHS Trusts to assume that year 2000 activities throughout the NHS would be financed from existing budgets, if necessary by postponing other projects or reducing resources devoted to them. They have recognised, however, that as the year 2000 approaches the costs of skilled assistance will increase and may be available only to those prepared to pay the premium. The Health Group of the Computer Software and Services Association (CSSA) have expressed concern about the capacity within the industry to supply additional resources to the NHS over and above those required to deal with the systems they have supplied. They have pointed out that demand in sectors such as Banking and Insurance is leading to a premium being added to fee rates increasing the costs of skilled assistance and reducing the availability of resources to the public sector. The NHS Executive however consider that this is unlikely to be a serious issue as the NHS generally do not buy in much external assistance as in the main they consider it not particularly cost effective.

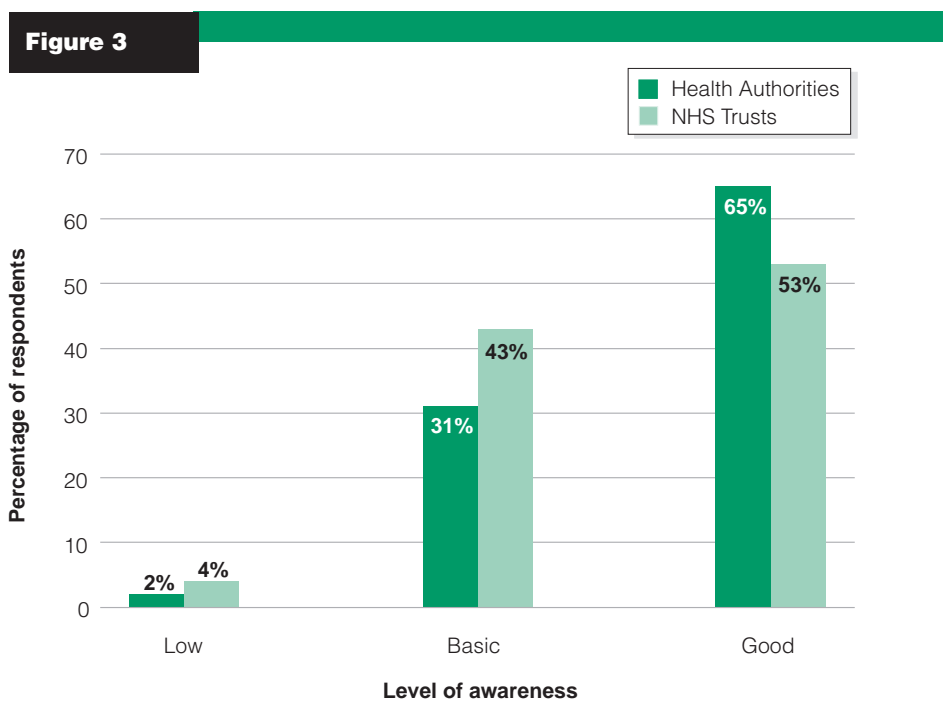
## Progress

**2.28** We surveyed all NHS Trusts and Health Authorities in October 1997 to establish what progress the NHS had made. 84 per cent of Health Authorities and 72 per cent of NHS Trusts replied to our survey. This survey was conducted around the same time as the second letter from the NHS Executive to Chief Executives was issued (paragraph 2.21) and responses therefore are unlikely to have taken account of the contents of this letter.

### Level of awareness

**2.29** The results of the survey show that at that time one third of Health Authorities and almost half of the NHS Trusts who responded to the survey considered there was not yet a good awareness of the importance of year 2000 issues in their organisation (Figure 3).

Percentage level of awareness of the importance of year 2000 issues at October 1997



**2.30** An example of how one NHS Trust approached the question of raising and maintaining awareness is shown in Box 1.

#### Box 1

University College London NHS Trust raised awareness of year 2000 issues by a concerted programme of presentations to managers and clinicians, through the Trust newspaper, through the e-mail system and by designating User Co-ordinators in all parts of the Trust.

The Trust is also placing stickers on all computer equipment and electromedical equipment. A yellow sticker confirms that the equipment is registered with the Year 2000 project, a red sticker identifies that action is required and a blue sticker signifies that the problem has been resolved.

This simple but effective approach ensures that all users are aware of the status and possible risk of using the equipment, but also acts as a highly visible reminder, maintaining the level of awareness of the year 2000 issue.

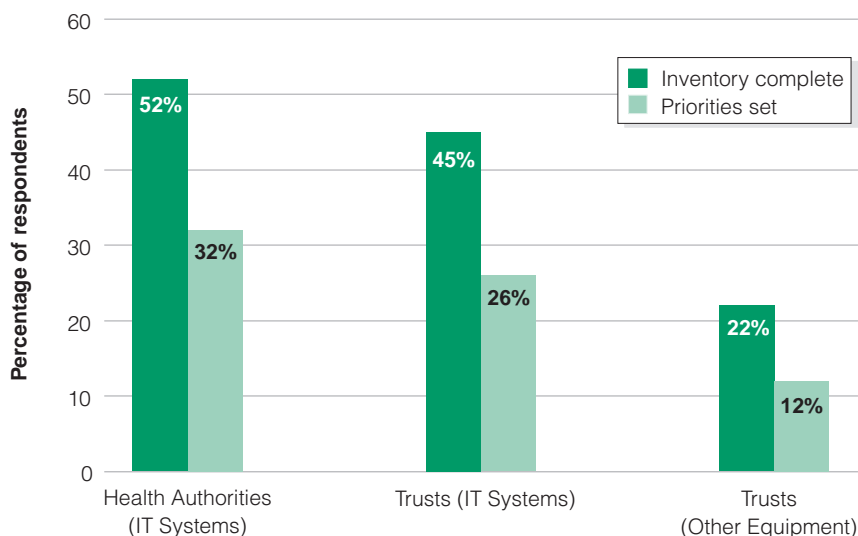
### Programme management

**2.31** The survey showed that in October 1997 52 per cent of Health Authorities and 45 per cent of NHS Trusts had completed their inventories of IT systems; 32 per cent of Health Authorities and 26 per cent of NHS Trusts had prioritised the importance of their systems.

**2.32** Progress on plans to deal with clinical and other equipment in NHS Trusts was less advanced with some 22 per cent having completed an inventory and 12 per cent finished the process of setting priorities (Figure 4).

Programme Management  
- stages complete

**Figure 4**



### Information from suppliers

**2.33** Around 60 per cent of NHS organisations who replied to our survey have received useful advice from suppliers. Some commented that they would have welcomed more help from the NHS Executive or NHS Supplies to avoid every NHS Trust and Health Authority asking each supplier for the same information. The Health Group of the Computer Software and Services Association have also suggested that a single NHS clearing house to handle enquiries and share experience could reduce the impact on both the NHS and suppliers and ensure that lessons learnt have been disseminated. This is now being undertaken mainly by

the Information Management Group's central team which set up a Helpline to handle enquiries and set up a world wide web site to share information; this resource provides a central supplier liaison and information dissemination service in addition to its other activities.

**2.34** About 10 per cent of organisations had completed their inquiries of suppliers. The Computer Software and Services Association were surprised by how few follow-up queries had been received from the NHS, even when answers to the questionnaires revealed non-compliant systems. An example of how one NHS Trust is approaching the issue of testing their IT systems is set out in Box 2.

### Box 2

Kings Healthcare NHS Trust has decided to carry out an in-house testing programme of their IT systems. Although systems will mainly be selected for testing on the basis of a risk assessment, some which have been declared compliant by their suppliers will be included. The reasons for this are:

- some suppliers failed to provide evidence to support their assertion that their products were year 2000 compliant;
- some systems may manage the year 2000 differently on different hardware and software configurations;
- some systems are so critical that the Trust is unwilling to rely solely on supplier assurances.

To test the systems, Kings Healthcare is creating an off-line situation which mirrors the real environment as closely as possible. This allows the computer's internal clock to be advanced without risk of corrupting the live system.

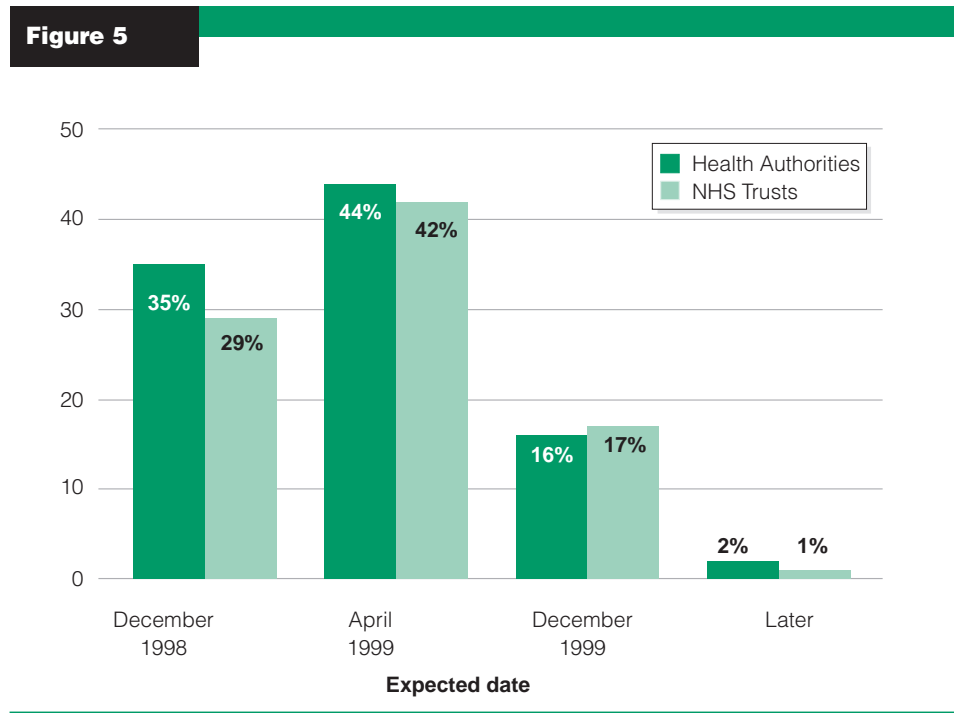
### Timescale

**2.35** The NHS guidance requires by 31 December 1998 that all critical systems should be ready and fully tested, or detailed plans have been made for coping without those systems or equipment that cannot be repaired or replaced in time. The key objective is that organisations will be ready for the millennium, equipped with compliant systems or able to manage the consequences of non-compliance.

**2.36** At the time of our survey in October 1997, less than a third of NHS Trusts who replied to our survey were predicting that their IT systems would be year 2000 compliant by the end of 1998 though NHS Trust responses may not have taken into account the NHS guidance on compliance issued in October 1997 (paragraph 2.21). Almost three quarters of the NHS Trusts thought they would be ready by the end of April 1999, but just under one fifth of NHS Trusts did not think that they would be able to achieve year 2000 compliance for their IT systems until the end of

1999, a timescale which leaves no room at all for any slippage (Figure 5). Just under 10 per cent of the NHS Trusts said they could not be confident of their ability to succeed in ensuring year 2000 compliance in time. Most NHS Trusts are almost entirely reliant on third party suppliers for sorting out their software packages and devices. Like many other users of IT equipment NHS Trusts' confidence in completing on time in most cases is dependent on their own confidence in their suppliers' ability to ensure year 2000 compliance. The picture for Health Authorities was broadly similar, but almost all Health Authorities were confident that they would be ready in time.

Expected date of completion for IT Systems reported in October 1997

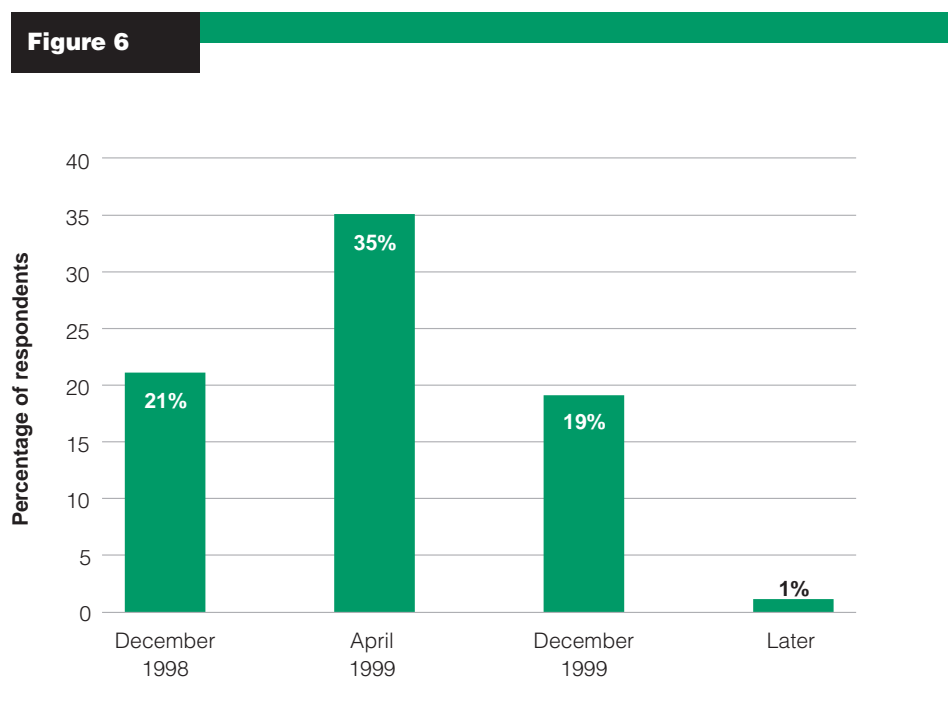


**2.37** NHS Trusts were somewhat less optimistic about the prospects of achieving year 2000 compliance for all their clinical equipment (Figure 6). Just over one fifth of them thought they would be ready by the end of 1998, with a further third considering that they would need up till the end of April 1999 to complete their programme. One fifth of NHS Trusts thought that they would need right up to the end of 1999 and 15 per cent of NHS Trusts were not confident that they would succeed in ensuring that their clinical equipment would continue functioning normally in year 2000. The likelihood of failure in medical devices is at present unknown. The NHS Executive consider that most Year 2000 project managers, coming from a traditional IT background, may be assuming medical devices suffer from the same error rates as software. In the view of the NHS Executive, this may be over pessimistic. Moreover, the NHS Executive's initial analysis of plans



produced in March 1998 suggests that NHS Trusts and Health Authorities have provisionally earmarked a total of £150 million for the replacement of non-compliant medical equipment, which is about half as much again as is normally spent each year.

**Expected date of completion for Clinical Systems in NHS Trusts reported in October 1997**



### Costs

**2.38** The NHS Executive told NHS organisations to assume that year 2000 activities should be financed from existing budgets, if necessary by postponing other projects or reducing resources devoted to them. Some non-compliant systems are already scheduled for replacement as part of existing IT investment programmes. Our survey asked NHS organisations to identify additional finance budgeted to complete their year 2000 programmes and resources transferred from other programmes. At the stage of the survey in October 1997, 43 per cent of NHS Trusts and 48 per cent of Health Authorities who replied were able to give initial estimates. If these are typical of the whole NHS, we estimate that the cost to the NHS of year 2000 activities in Health Authorities and NHS Trusts is likely to be around £170 million. In addition to this an estimate commissioned by the NAO which extrapolated from available published information suggests that remedial costs for GP systems could be in the range of £60 million to £120 million. These

figures, however, need to be treated with caution as NHS organisations did not have to produce costed plans until 31 March 1998. The experience of many other organisations has been that initial estimates rise when more detailed plans are produced.

**2.39** We also asked NHS organisations to identify the biggest year 2000 related problem they faced. The single largest category of comments related to the difficulties NHS organisations anticipated in providing adequate resources for their year 2000 programmes. The NHS Confederation have said that while diverting funding to year 2000 work would not have a direct effect on clinical practice, without the availability of additional resources, there would be consequences for other projects dependent on capital investment, such as the move to single sex wards.

**2.40** Research by Cap Gemini has identified the average cost of achieving year 2000 compliance in medium and large organisations (Figure 7). An average NHS Trust employs around 2,000 staff and would be considered by Cap Gemini as a large organisation. Most NHS Trusts are not extensively computerised however, and an alternative comparison may be with medium sized commercial organisations, but Cap Gemini consider that the more appropriate comparison for most NHS Trusts is with large organisations. They point out that, within this category, most public sector organisations are at the lower end of the range, spending on average 28 per cent of their annual IT budget on year 2000 issues, compared with an average of 71 per cent in private sectors.

**Estimated average cost  
of achieving Year 2000  
compliance**



Source: Cap Gemini

**2.41** Figure 8 shows the estimated total cost to the NHS of achieving year 2000 compliance if the Cap Gemini averages apply to all NHS Trusts and Health Authorities. This is compared with the estimated total cost derived from our survey, which is at the lower end of the range of costs in other organisations.

**Estimates of costs to the NHS achieving Year 2000 compliance**

**Figure 8**

Estimated cost of NHS organisations as large organisations (over 500 employees) <sup>1</sup>	£850 million
Estimated total cost of NHS organisations as medium sized organisations (150-499 employees) <sup>2</sup>	£200 million
Estimated total cost from NAO survey	£170 million

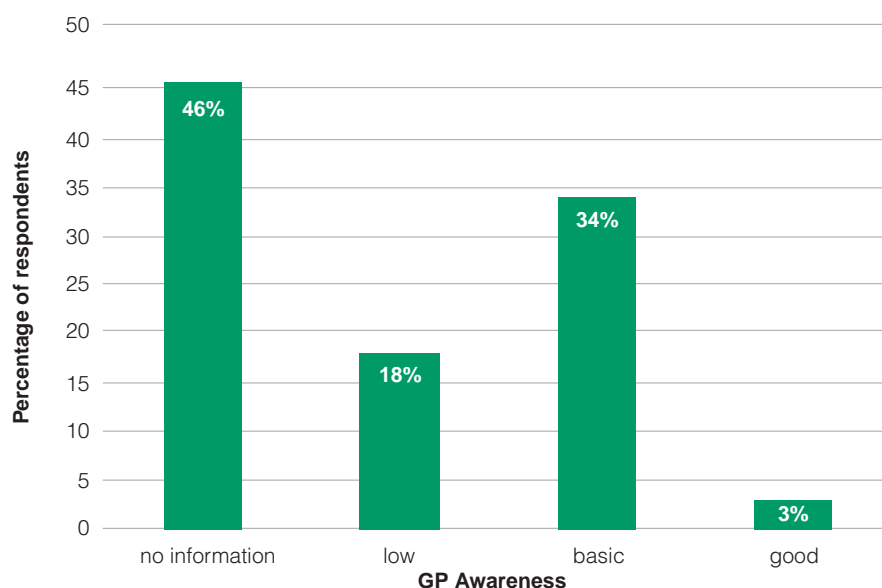
- Notes: 1. This estimate applies the Cap Gemini average cost of a large organisation (£2 million) to all NHS Trusts and the average cost of a medium size organisation (£400,000) to all Health Authorities.
2. This estimate applies the Cap Gemini average cost of a medium sized organisation to all NHS Trusts and Health Authorities.

**General practice**

**2.42** Information about the position of General Practitioners has been more difficult to obtain as just under half of Health Authorities (44 per cent) reported in our survey that they had not yet collected information on GP practices in their area. Almost all Health Authorities (92 per cent) considered that there was not a good level of awareness on year 2000 issues amongst GPs and nearly a third (32 per cent) assessed it as low (Figure 9). Almost one third (31 per cent) of Health Authorities said they were not confident that GPs’ systems would be year 2000 compliant in time. An example of how one Health Authority raised good awareness on the part of GPs is shown in Box 3.

**Health Authority assessment of GP awareness at October 1997**

**Figure 9**



### Box 3

Bexley and Greenwich Health Authority held a series of evening seminars at which 70 per cent of GPs attended. These seminars were recognised as counting towards GPs' obligations to keep up to date through postgraduate medical education. Practice managers also attended these seminars.

The Health Authority engaged the National Computing Centre Ltd to work with 10 volunteer practices assessing the problem and developing an implementation plan. This informed the Health Authority's strategic planning and provided considerable benefit to the GP practices.

The Health Authority has used the year 2000 issue as a way of further developing working relationships and co-operation between GPs, Health Authorities and the local Trust.

**2.43** Health Authorities use an IT system developed by Family Health Systems, an agency of the NHS Executive, to manage 16 million registrations of patients with GPs each year, administer screening invitations to around 1.8 million women, and manage payments to GPs of around £5,000 million annually. Work on this system began in 1995 to ensure that the call and recall cycles for screening services would operate correctly beyond 1999. In February 1997 a full assessment of the system was carried out and work to modify and test the system began in June 1997. Family Health Service makes two standard releases of software to users each year. They plan to release year 2000 compliant software in June 1998 and February 1999.

**2.44** The remedial work for systems in GP practices is the responsibility of individual GP practices with advice and support from the Health Authorities. There have been a large number of different suppliers of GP systems, but most GPs have bought their systems from a few major suppliers. All of these major suppliers have programmes underway to ensure year 2000 compliance and at this stage, it appears likely that they will succeed. Six GP systems have so far been tested and accredited by Family Health Systems as year 2000 compliant. There may, however, be more problems with the smaller suppliers who have supplied systems to about 25 per cent of GP practices. The Health Group of the Computer Software and Services Association were not wholly confident about the ability of some smaller suppliers to achieve year 2000 compliance. In some areas GPs may be forced to replace their existing systems. From early 1998 General Practitioners have only been reimbursed the costs of purchasing systems which were year 2000 compliant.

## Conclusions

### How well has the programme been managed?

**2.45** Initially the approach taken by the NHS Executive was to set up a small project team within the Information Management Group to assess the impact of the millennium date change. They alerted the NHS to the problem but did not set targets, and considered that there were unlikely to be serious problems with equipment.

**2.46** In common with many organisations, as more information became available, there was a growing realisation of the seriousness of the problem. In 1997 the NHS Executive took a much stronger line establishing targets for action, clear accountability for results, strong senior management leadership and close monitoring.

**2.47** The framework of a well managed project is now in place. The size and complexity of the programme is such that very tight control will be required at all levels to ensure success. The NHS Executive is assisting NHS organisations by sharing experience which should avoid duplication of work in every Health Authority and NHS Trust.

### Will NHS Trusts and Health Authorities be ready on time?

**2.48** The timetable set by the NHS Executive allows 9 months from completing detailed plans and budgets in March 1998 to all critical systems being ready and fully tested, or detailed plans made for coping without these systems or equipment that cannot be repaired or replaced in time, by 31 December 1998. Our survey in October 1997 showed that one fifth of NHS Trusts and Health Authorities thought they would need right up to the end of 1999 to ensure all their IT systems were year 2000 compliant and 10 per cent of NHS Trusts were not confident that they would be successful.

**2.49** NHS Trusts who do not receive a prompt satisfactory response from clinical equipment suppliers on the timescale set by the Medical Devices Agency are unlikely to have available the information they require to even complete their detailed plans by 31 March 1998. Our survey showed that, 15 per cent of NHS Trusts were not confident they would succeed in ensuring that all their clinical equipment continued functioning normally in the year 2000.

**2.50** Research undertaken by Cap Gemini, a leading European computer services and business consultancy, showed that, on average, it will take public and private sector organisations with more than 500 employees two and a half years to resolve the Year 2000 problem. If this average applies to the NHS, work should have started in July 1996 to meet the NHS Executive deadline of having all critical systems ready and fully tested, or detailed contingency plans in place, by 31 December 1998. They were first given formal notice that they had to do so in September 1996. Therefore many NHS Trusts and Health Authorities will need to work significantly faster than other large organisations to complete their year 2000 compliance programmes by that deadline. The British Computer Society has advised organisations undertaking year 2000 programmes to be pessimistic about the chances of success until they have good reason to be otherwise.

**2.51** Considerable efforts are now being made by the NHS and a well considered project framework is now in place. However the NHS Executive has set NHS Trusts a timetable which is challenging in comparison with estimates from a range of public and private organisations of the time required to complete Year 2000 projects by 31 December 1998. From our survey it is clear that NHS Trusts have concerns about being able to meet that timescale and we conclude that some parts of the NHS remain at risk of failing to achieve year 2000 compliance. The NHS Executive have told us however, that their strategy has all along anticipated having this opportunity of a further 12 months before the turn of the Millennium itself to react should particular problems arise.

### **Will General Practitioners be ready?**

**2.52** The limited information available at present on the state of readiness in General Practice suggests that as a body GPs are likely to have difficulty in achieving compliance. Although individual GP practices should not present particularly complex problems and the major suppliers have year 2000 compliance programmes in hand, the sheer numbers involved, the range of systems in use and the difficulty of ensuring that action is taken by every GP, present a challenge to all concerned, including the NHS Executive.

**2.53** Almost all Health Authorities considered that there was not a good level of awareness among GPs of year 2000 issues, and almost one third did not have confidence that GP systems would be year 2000 compliant in time. These assessments indicate that there is a need to do more to increase awareness of the issues amongst GPs, particularly in relation to the potential equipment failures, and to increase efforts aimed at encouraging all GPs to develop a year 2000 action plan by March 1998.

### How much will it cost?

**2.54** NHS organisations have been told by the NHS Executive that they should plan to meet the cost of their year 2000 compliance programme from within existing budgets. The NHS Confederation have expressed concern about the possible diversion of funds away from other capital projects.

**2.55** If the estimates of NHS organisations in a position to reply to our survey apply to the whole NHS, the cost of year 2000 programmes is estimated to be in the order of £170 million. The cost of ensuring GP systems are year 2000 compliant could add at least another £60 million, giving a total estimate of £230 million for the whole NHS. This is at the lower end of the range of costs for similar organisations.

**2.56** Inadequate resourcing increases the risk of failure, and the single largest area of concern identified by respondents to our survey was about the difficulties they anticipated in providing adequate resources. The NHS Executive have warned that the cost of skilled assistance on year 2000 projects is increasing and availability is reducing. This will put further pressure on year 2000 project budgets, to the extent that external assistance is required.

## Recommendations

**2.57** The NHS Executive should continue to monitor progress very closely, taking immediate action if necessary, to ensure that all Health Authorities and NHS Trusts successfully complete all elements of the project, and facilitate the exchange of information and experience.

**2.58** The NHS Executive should consider the need for further selective direct intervention in those cases where progress reports from NHS Trusts and Health Authorities indicate a risk of failing to achieve year 2000 compliance, or inadequate contingency plans to cope with failures in systems or equipment.

**2.59** The NHS Executive and Health Authorities should increase efforts to inform GPs of the full consequences of year 2000 problems and through stringent monitoring assure themselves that GP services will not be disrupted by the year 2000.

**2.60** The NHS Executive should regularly review the need for further investment of resources in year 2000 projects in the light of progress reports from NHS Trusts and Health Authorities.



# Part 3: Year 2000 compliance in the Department of Social Security

## Summary

**3.1** This part examines the risks faced by the Department of Social Security, the action they have taken to deal with the millennium threat and progress so far.

**3.2** Our findings are that the Department established in September 1996 an effective project management structure with a high level Project Board, reporting directly to the Departmental Board, to advise, monitor and co-ordinate the work of project teams which were established within each of the Department's Business Units. A clear timetable was established and progress monitored with regular reports to senior management. The management structure was further strengthened in January 1998 with the appointment of a senior level Programme Manager and the formation of a Programme Steering Group chaired by the Chief Executive of Information Technology Services Agency. The year 2000 compliance programmes of software suppliers and IT contractors are being monitored closely. In general the targets set out in the project plans have been met, and where any slippage has occurred this has been identified and dealt with promptly. In February 1997 the Department estimated the cost at £30 million. By November 1997 when detailed costed plans had been produced, estimated costs had risen to £45 million.

**3.3** Our assessment is that, providing the Department continue their current approach of tight project management and close monitoring, they are on schedule to achieve compliance by their target dates.

## Introduction

**3.4** The Department is responsible for the development and delivery of an efficient, modern Social Security programme. Its objectives are to treat all benefit recipients consistently and fairly, ensuring that they are paid the correct entitlement at the right time, informing prospective recipients of possible eligibility whilst protecting the rights of National Insurance contributors and taxpayers.

**3.5** The Department employ 99,000 staff based in 1,060 of their own offices and many Employment Services offices using one of the largest civilian computer operations in Europe to process benefits for 30 million clients. Expenditure in 1996-97 was £96 billion.

## **Risks to the Department of Social Security**

### **IT systems**

**3.6** The core business of the Department is the payment of non-contributory benefits, contributory benefits and pensions, and the stewardship of the National Insurance receipts. These are all based on large complex mainframe computers processing enormous quantities of data and linked by some 3,600 computer servers to 63,900 terminals in hundreds of geographically spread offices. Some of these systems have been computerised since the early 1970s, whilst others, such as the Job Seekers Allowance implemented in 1996, were introduced much more recently. A failure of these huge mainframe systems could result in benefits not being paid, inaccurate records or delays in payment of benefits.

**3.7** In addition to the computer terminals, there are also some 71,300 personal computers (PCs) – the vast majority of which are also linked to the mainframe or server systems. Some of these PCs are used to access a variety of support systems. Whilst not critical to the core business, many of the important management control functions rely on these systems. Failure of these systems would impair day to day operations of the Department.

### **Electronic equipment**

**3.8** The Department have also identified the need to ensure that equipment containing microprocessors is year 2000 compliant. This type of equipment can be found in air-conditioning plants, lifts and security systems. Failure of this equipment could disrupt normal operations, but is unlikely to put the core business at risk.

## Responsibility for achieving year 2000 compliance

**3.9** Working within the overarching Programme structure, the individual Business Units have prime responsibility for compliance activity within their Unit. The individual units of the Department include:

- Headquarters - supports Ministers on both policy and legislation, and provides administrative services to the Agencies.
- Contributions Agency - ensures compliance with National Insurance law, maintains NI records and provides NI information to other DSS Agencies.
- Benefits Agency - assesses, delivers and administers most social security benefits.
- War Pensions Agency - delivers benefits and other services to war pensioners.
- Information Technology Services Agency - provides, regulates and controls IT services, either direct or through external contractors, for the delivery of the DSS programme.
- Child Support Agency - is responsible for the assessment and collection of child support maintenance.
- Independent Statutory Bodies, e.g. Office of the Pensions Ombudsman.
- Non-Departmental Public Bodies e.g. Occupational Pensions Regulatory Authority (OPRA).

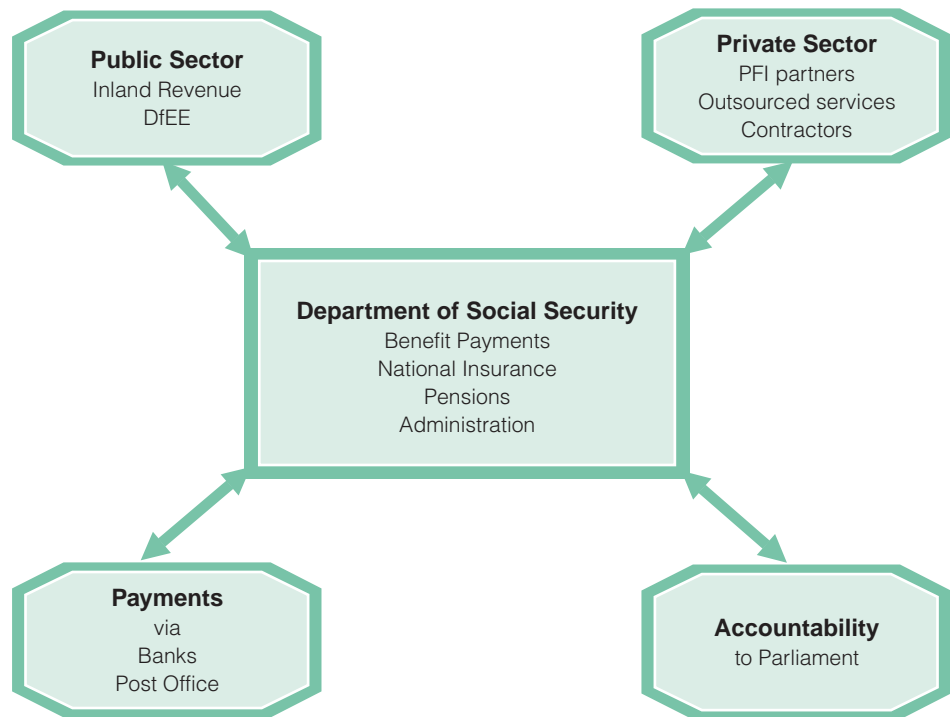
The Department also works closely with the Northern Ireland Social Security Agency, and with the Employment Services Agency because of the high degree of interworking between the Employment Service and the Benefits Agency.

**3.10** All the Business Units also have links with external partners which provide and receive information from the Department. For example other government departments, such as the Inland Revenue pass to the Department information which is used to calculate benefits. Similarly other organisations such as commercial banks and Post Offices are involved in payments of benefits.

**3.11** Several of the Department’s functions have been contracted out to the private sector, including much of its computer processing and some computer system development work. The replacement of the National Insurance Recording System, was the first information systems development project to be contracted through the Private Finance Initiative. Figure 10 shows the links between the DSS and other organisations which are critical to the functioning of the social security programme.

**Links between DSS and other organisations**

**Figure 10**



**Action taken**

**3.12** The Departmental Board established a year 2000 Project in September 1996 which is managed by the Information Technology Services Agency but is responsible for all year 2000 issues across the Department. The Project Board provides direction and management of the year 2000 project within the Department, ensuring that the central project is on course, providing decisions on major issues, arbitrating on any scheduling or prioritisation dispute and ensuring that all areas within the Business Units are addressing year 2000 issues.

**3.13** The Project Board comprises senior representatives from the Business Units and reports directly to the Departmental Board on which the Departmental Accounting Officer and Agency Chief Executives sit. This enables senior management to be aware of the issues and ensure that action to achieve year 2000 compliance has the necessary priority. Monthly progress reports were issued by the Project Board to the Information Technology Services Agency's Chief Executive's Management Team.

**3.14** In January 1998 at the start of the more intensive phase of implementation and delivery, the management was further strengthened by the appointment of a senior level Programme Manager and the introduction of a Programme Steering Group attended by Board level representatives from the Executive Agencies and chaired by the Chief Executive of the Information Technology Services Agency. Progress reports are now issued to this Steering Group under the new programme structure.

**3.15** The Department decided to manage the Year 2000 Programme using the CCTA recommended project management methodology, PRINCE. This enables the Department to initiate, plan, control and monitor the project in line with best practice. The four stages of the central project are shown in Box 4.

**Main Stages of the DSS  
Year 2000 Project**

**Box 4**

**Stage 1 - Initiation (July 1996 to September 1996)**

Set up project, publicise it, produce Information Packs for Business Units, commence Year 2000 database, etc.

**Stage 2 - Analysis (September 1996 to August 1997)**

Problem identification and impact analysis. Monitoring the commencement of problem resolution.

**Stage 3 - Major Issue Resolution (September 1997 to August 1998)**

Co-ordination and collation of Business Unit feedback on the changes required and undertaken to the major IT systems to ensure that compliance timetable is met. Implementation of remedial work.

**Stage 4 - Monitoring and Assurance (September 1998 to April 2000)**

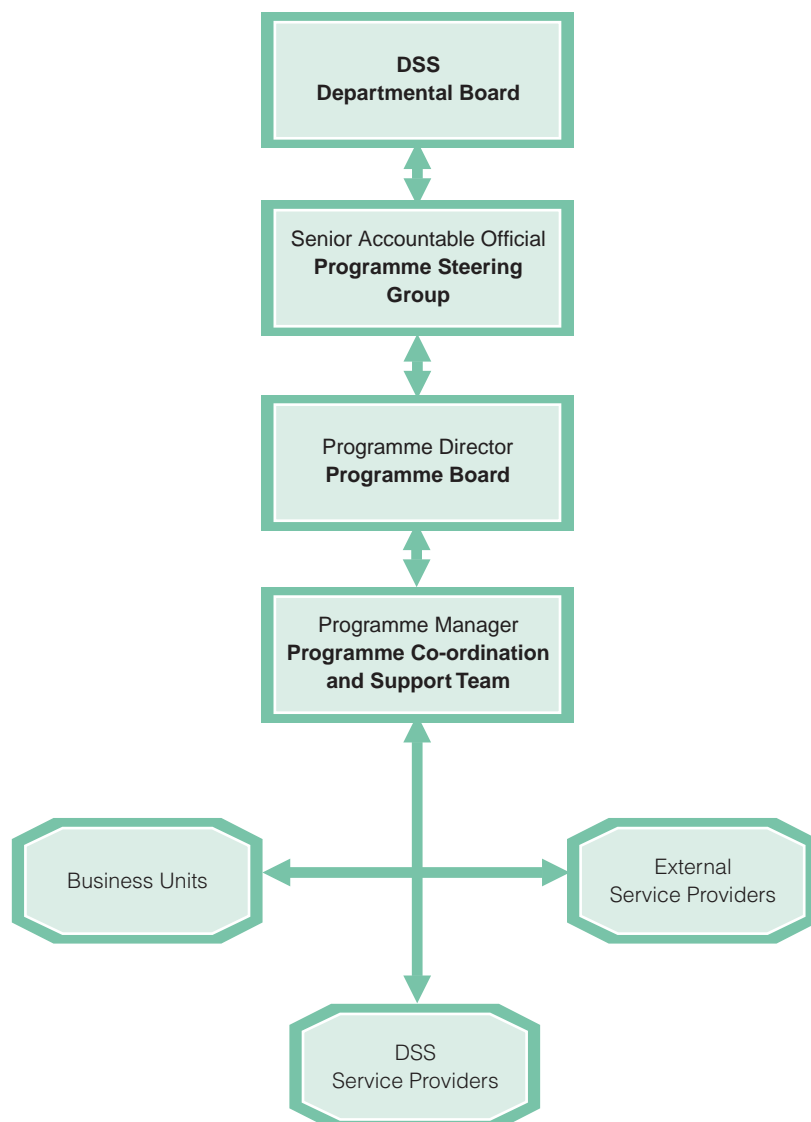
Maintain a watching brief as major systems operate through an annual cycle prior to the millennium change.

**3.16** The central programme team is responsible for achieving progress and ensuring that targets are met. The actual compliance work is carried out by the Business Units, the Information Technology Services Agency, and companies providing outsourced services to the Department. Each Business Unit within the

Department also has established a project team steering the action requiring to achieve year 2000 compliance. These project teams work closely with the year 2000 Programme and receive frequent advice and guidance from the programme team. Figure 11 shows the programme structure adopted by the Department.

**DSS Year 2000 project structure**

**Figure 11**



**3.17** The project teams have adopted the triage methodology endorsed by the British Computer Society Year 2000 Working Party, details of which are shown in Box 5. The whole approach and plans have been audited by the Departmental Information Systems Audit and by KPMG, an independent consultancy and audit company.

### Triage Methodology

#### Box 5

The triage methodology is an approach to prioritising the work which needs to be done. The Information Technology Services Agency undertook a full analysis of all the mainframe and support systems considered critical to the core business of the Department. For each system the first date when a module of the system might fail was identified. For some modules this was 1 January 2000, but for many others the first fail date was earlier, with some as early as 1 January 1998.

The Information Technology Services Agency developed a project plan which enabled them to give priority to the modules with earlier fail dates. This ensures that scarce resources are used effectively and, through careful progress monitoring, that the necessary modifications to modules are made and tested before their earliest fail date arrives.

**3.18** The key milestone targets are:

- 31 August 1998: Major business applications (except Job Seekers Allowance Payment System) confirmed as compliant.
- 31 October 1998: Job Seekers Allowance Payment System confirmed as compliant.
- 31 March 1999: Business-critical infrastructure components confirmed as compliant.  
Important, but not critical, applications confirmed as compliant.
- 31 August 1999: Important, but not critical, infrastructure components confirmed as compliant.

## Progress

**3.19** Each Business Unit has carried out a thorough and comprehensive survey of all systems and identified those mainframe systems which are considered to be critical to the core business of the Department. The Departmental Information Technology Authority produced five reports in 1996 covering hardware and operating systems, Departmental infrastructure, Departmental applications, third party products and a management summary. These provided an excellent analysis of the problem and the effect on the Department.

**3.20** Registers and inventories of all external sources and destinations of data are being compiled by the Information Technology Services Agency and the Business Units. This will ensure that all links between internal and external systems can be identified and checked. The Information Technology Services Agency have also established a database of all IT contracts and have examined all contracts to identify if they are year 2000 compliant. They established at the beginning of January 1998 that 104 of the 141 major IT contracts (74 per cent) were year 2000 compliant. The remaining 37 contracts are being renegotiated to ensure they are year 2000 compliant. Of these, 23 are telecommunications contracts which the Information Technology Services Agency expect to achieve compliance in 1998. So far renegotiation of the contracts have not led to any increase in costs.

**3.21** Stage 2 of the Year 2000 Project called for the analysis phase to be completed by August 1997. Most of this was completed on time with each Business Unit producing a plan setting out details of the timetables, costs and status of the tasks necessary to achieve compliance. These plans have been amalgamated into a Departmental Compliance Plan against which progress is being monitored centrally. Where there was any slippage, for example when the Benefits Agency Estates did not fully meet the timetable, the issue was escalated through the Benefits Agency line management and the Benefits Agency Year 2000 Project assumed an active management role. The Information Technology Services Agency has already begun testing the most critical systems and some, such as the system for the Disability Living Allowance have already been changed and tested.

**3.22** There are also hundreds of systems some of which are networked and some of which produce important financial and management information across the Department. These include applications for ordering supplies, maintaining inventories, car fleet monitoring and security breach monitoring. These are all termed Stand Alone Support Applications and most were developed in-house by the Information Technology Services Agency.



**3.23** On 1 November, the Information Technology Services Agency awarded a contract to a contractor, SEMA, for the support development and management of the majority of these Stand Alone Support Applications systems. SEMA are contractually responsible for ensuring year 2000 compliance for these systems and their progress is monitored closely by the appropriate project team. 10 systems were not transferred because of commercial sensitivity and these are still supported by the Information Technology Services Agency, who are currently re-writing these remaining systems to ensure year 2000 compliance.

**3.24** The final deadline for the Stand Alone Support Applications, which are less critical than the core business systems is to be year 2000 compliant by 31 March 1999. If work on these systems slips and compliance is not fully achieved, the management and control of day to day operations would be impaired, but in most cases the DSS could still pay benefits, though there could be delays in processing changes to benefits and in dealing with queries. To minimise these risks the Department has adopted a triage methodology, grouping the systems into four bands. This gives higher priority to systems which are more critical to the business.

### **Supplier information**

**3.25** The Information Technology Services Agency wrote to the suppliers of 1076 software packages. By the beginning of January 1998 replies had been received in respect of 477 packages, a response rate of 44 per cent. At that stage all the Business Units were satisfied that no replies were outstanding from suppliers of business-critical products. The Department, therefore, is confident that they have obtained all the compliance information there is available for all commercially supplied business-critical software. This information, however, is not yet sufficient to assure the Department that all such software will be compliant within the timescales.

### **Information exchange with third parties**

**3.26** There are a number of other organisations on whom the Department rely for various aspects of data processing. The Department is monitoring the progress external contractors are making on their own year 2000 programmes to ensure they will meet the Department's deadline of August 1998 for the compliance of its major systems.

**3.27** For example, the Department have a contract with EDS, a commercial computer services company to support the IT systems of the Child Support Agency. The Child Support Agency Year 2000 Project Team, in conjunction with the Information Technology Services Agency Contract Management Team, are monitoring the work carried out by EDS to make the system they support year 2000 compliant. Representatives of the project teams and EDS meet regularly to monitor progress and the central programme team receives a monthly update on progress.

### **Costs**

**3.28** In February 1997 the Department told the Social Security Committee that they estimated the cost of achieving year 2000 compliance was £30 million. The business-critical mainframe and infrastructure systems required £5 million to achieve compliance, with the remaining £25 million being required to replace personal computers and upgrade software.

**3.29** Since then each Business Unit has produced a costed business case. The Departmental Board, in the knowledge that funding for year 2000 compliance work has to be met from within allocated resources, encouraged managers to refine their estimates and restrict year 2000 changes to those which are critical to their businesses. The business cases were scrutinised within each Agency, and again at Departmental level.

**3.30** The individual plans were collated into a Departmental Business Plan which was approved by the Treasury in January 1998. The total cost of achieving year 2000 compliance is now estimated to be £45.7 million. The increase in the estimate from £30 million to £45.7 million arose mainly from a reassessment of critical hardware components which concluded that some 1600 communication servers could not be made compliant; they are being replaced by around 1430 new servers.

## **Conclusions**

**3.31** The Department have taken steps to ensure a co-ordinated approach is adopted by setting up dedicated project teams within each Business Unit, monitored and co-ordinated by a central Programme Board reporting through a senior Programme Steering Group to the Departmental Board. The approach to project management complies with best practice recommended by CCTA.

**3.32** Progress is being monitored with regular reports to senior management and the projects generally seem to be on target. Where there has been slight slippage, for example on the Benefits Agency Estates Project, this was detected quickly, and action taken to resolve the problem.

**3.33** The Department has established a database of all IT contracts and is closely monitoring the progress external companies are making on their year 2000 programmes. They have also contacted all software suppliers to check year 2000 compliance of the products used by the Department. At this stage the Department have no reason to believe that external suppliers and contractors will present them with any difficulty in meeting their target to have all business-critical applications compliant by August 1998.

**3.34** The Department of Social Security has now entered one of the more difficult phases of the programme in which all the changes required to ensure compliance have to be made. On the business critical mainframe systems, the Department has a clear plan to achieve compliance by August 1998 except for the Job Seekers Allowance Payment System where the target is October 1998. At the end of 1997 they were on target and providing they continue to manage the programme carefully, they are on schedule to achieve compliance by the target dates. The massive implementation programme to upgrade or replace the servers, personal computers and associated software throughout the Department's and Employment Services' offices will pose significant planning, logistical and management challenges, and presents a real risk to the Department because there is little room for any slippage. The Department has prioritised this work according to the impact on the business and has a target of completing the work by March 1999, leaving a contingency period from April 1999 to August 1999 to resolve any unforeseen issues.

## Recommendation

**3.35** The Department of Social Security should continue their well structured approach to achieving year 2000 compliance, monitoring progress closely and taking immediate remedial action if timetables slip.

# Appendix 1

## Potentially critical dates which some systems may fail to manage correctly

Date	Reason for failure
9 September 1999	9999 has been used by some IT systems to indicate "end of file"
31 December 1999 / 1 January 2000	Century rollover
29 February 2000	Leap day
31 December 2000	366th day of 2000
29 February 2004	Leap day

Source: Science and Technology Committee Report "The Year 2000 - Computer Compliance"

## **Appendix 2**

# **Co-ordinating Government response to the year 2000**

### **Role of the Central Information Technology Unit prior to 30 March 1998**

The Chancellor of the Duchy of Lancaster has an overall strategic and policy role in the approach central government departments and agencies take to resolve the Year 2000 problem. His role is to take an overview of progress, determine necessary action and to provide guidance. He is supported on this by the Central Information Technology Unit (CITU) in the Cabinet Office (OPS).

CITU and the Central Computer and Telecommunications Agency (CCTA) advise Departments, disseminate best practice and keep in touch with industry and other practitioners. CITU and CCTA have set up an inter-departmental group on year 2000 issues, and have been in regular contact with the Department of Trade and Industry, NAO, Taskforce 2000 and now Action 2000, the Computing Services and Software Association (CSSA) and the private sector so as to keep themselves fully up to date.

The principal responsibility for ensuring that computer systems are year 2000 compliant rests with individual departments. They are also responsible for ensuring that organisations in the wider public service sectors that they sponsor (such as local authorities, health authorities and non-departmental public bodies) understand their responsibilities, and that they need to ensure that their own respective computer systems are year 2000 compliant.

### **New year 2000 Unit**

On 30 March 1998 the Prime Minister established a new Year 2000 Unit as part of the Central Information Technology Unit in the Cabinet Office. The purpose of the new unit is to support the Ministerial Group on the Millennium Date Change (MISC 4) and its public sector sub group, in driving action across the public and the private sector, to prevent damage from the year 2000 date change. It will co-ordinate and monitor across the whole public sector, and will work with Action

2000 and key parts of central government. It will not affect the responsibilities of Departments for getting their own house in order and mobilising the public sector bodies for which they are responsible, or the work of DTI and Action 2000 with the private sector.

The new unit will manage cross-departmental pieces of work, such as the assessment of risks to the infrastructure which has been commissioned by MISC 4; co-ordinate presentation to Parliament and the media of the action the Government is taking, across the public and private sector; work with the Foreign Office, Ministry of Defence, DTI and European and Overseas Secretariats to ensure that efforts overseas fit smoothly with work at home; and support the work of MISC 4 and the sub group on ensuring the compliance of key areas of the national infrastructure.

The unit will report to the President of the Board of Trade as chair of MISC 4, and to the Chancellor of the Duchy of Lancaster as chair of the public sector subgroup.

## Appendix 3

# Departments and Agencies making returns

Department	Agency(ies)
Cabinet Office	<i>Buying Agency Civil Service College Government Car &amp; Dispatch Agency Property Advisors to the Civil Estate Security Facilities Executive</i>
Department of Culture Media & Sport	<i>Historic Royal Palaces Royal Parks</i>
Department for Education & Employment	<i>Employment Service Agency</i>
Department for International Development	
Department for Environment Transport and the Regions	<i>Coastguard Agency Driving &amp; Vehicle Licensing Agency Driving Standards Agency Highways Agency Marine Safety Agency Planning Inspectorate Queen Elizabeth II Conference Centre Vehicle Certification Agency Vehicle Inspectorate</i>
Department of Health	<i>Medical Devices Agency Medicines Control Agency NHS Estates NHS Pensions Agency</i>
Department of Social Security	
Department of Trade & Industry	<i>Companies House Employment Tribunals Insolvency Service National Weights &amp; Measures Laboratory Patent Office Radiocommunications Agency</i>
Export Credits & Guarantees Department	
Foreign & Commonwealth Office	<i>Wilton Park</i>
Forestry Commission	
Government Offices	

continued ...

<b>Department</b>	<b>Agency(ies)</b>
HM Customs & Excise	
HM Land Registry	
HM Treasury	
Home Office	
Inland Revenue	<i>Valuation Office</i>
Intervention Board	
Government Property Lawyers	
Treasury Solicitors	
Lord Advocate's Department	<i>Crown Office for Scotland</i>
Lord Chancellor's Department	<i>Courts Service</i> <i>Public Trustees Office</i>
Ministry of Agriculture Fisheries and Food	
Ministry of Defence	
National Savings	
Office of National Statistics	
Ordnance Survey	
Public Record Office	
Royal Mint	
Scottish Office	<i>Registers of Scotland</i> <i>Scottish Agricultural Science Agency</i> <i>Scottish Court Service</i> <i>Scottish Prison Service</i> <i>Scottish Record Office</i>
Welsh Office	