COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 02.06.1999

COM(1999) 275 final

REPORT

TO THE EUROPEAN COUNCIL - COLOGNE, JUNE 1999

FROM THE EUROPEAN COMMISSION

ON

THE "MILLENIUM BUG": THE PREPAREDNESS OF KEY EU INFRASTRUCTURES FOR THE Y2000 DATE CHANGE

Introduction

The Commission adopted on 2nd December 1998 a report on **"How the EU is tackling the Year 2000 Computing Problem"** (Y2K), which was presented to the European Council in Vienna. The purpose of the Communication was to provide an overview of Member State preparations and progress in addressing this problem and to identify the areas where progress may have been inadequate and action needed to be taken.

The Vienna European Council subsequently requested the Commission to *"convene a meeting of representatives of the public infrastructure providers from the Member States to* ***establish whether the cross-border dependencies within the EU in areas such as transport, energy, and water supply are being adequately addressed and to recommend appropriate action where required to the next European Council***".

This Report responds to this mandate. In doing so, it recognises that any assessment of the potential cross-border impact of the Y2K issue must take as its starting point the level of preparedness in and between sectors at a national level, as well as the availability of verified and authorised information. Additionally, the report looks beyond the Union's borders to those areas and countries where the effect of the Y2K issue has the greatest potential to impact on the situation of the EU itself.

Whilst intensive work has been on-going on the Y2K issue in most areas over the last 18 months, it is clear that a further intensification of efforts is required by the private sector, and by governments and other public institutions across the European Union.

The situation in general

Around the globe, the Year 2000 (Y2K) issue is being addressed by governments, industry, and international organisations with increasing attention and resources. It is estimated by experts that 1 trillion euro has already been spent worldwide to investigate, rectify, test, and audit IT systems. The G8 World Economic Summit in Cologne in June is expected to discuss it as a major issue for the increasingly networked global economy.

In the European Union, the Commission has continued to convene meetings with national and sectoral experts from the Member States to exchange information on progress and experiences.

The Commission hosted a two-day meeting of EU public infrastructure providers in April 1999, during which:

- the situation of key EU infrastructure sectors was investigated in terms of preparedness for the roll-over to the next millennium;
- areas were identified where significant cross-border and cross-sector dependencies exist;
- and the extent to which these dependencies are being addressed was identified.

A more detailed analysis is attached in annex to this Report.

At the Telecommunications, Industry, Energy, Transport, and Internal Market Councils a consensus has emerged on the importance and urgency with which this matter needs to be addressed.

Positive developments

Although the situation varies between sectors and in different countries, a number of **important trends are now emerging across all infrastructure sectors**, and throughout the EU as a whole. **Positive** developments are:

- *Regulatory and supervisory authorities are increasingly involved in monitoring and auditing vital infrastructure sectors.*
- *Co-ordination efforts are being carried out by sectoral, national, and international associations.*
- *Bilateral, multilateral, end-to-end, and national testing is occurring.*
- *Information campaigns are being planned or ongoing to maintain public confidence.*
- *Greater information on progress, results, risks, and contingency plans is available.*

Interdependencies

The Year 2000 computing (Y2K) problem however, is not simply an information technology (IT) system problem, but also **concerns a number of key sectorial interdependencies of processes**. These interdependencies exist at many levels, **the most fundamental of which are those basic infrastructures which provide the essential services** upon which all the sectors depend. The telecommunications sector depends on electricity and water. The energy sector on telecommunications and water. The gas sector on electricity, etc. Disruptions in one sector could have a cascading effect on others.

Many organisations completing their Y2K adaptation and testing activities are already shifting their efforts to contingency planning. Their scope of interest is becoming much wider than their own internal environment, including the need to assess the effect of external factors. Inevitably, concerns arise regarding the **preparedness of the suppliers of essential services, in particular, areas such as energy, transport, telecommunications, finance, and water**.

Reasons for concern

The situation within the European Union and country attitudes to the problem are neither consistent nor homogeneous, so generalisations should be avoided. Furthermore, the public institutions do not have, and are unlikely ever to have, full information to be able to make reasonable comparisons between countries or sectors.

Although steady progress is being reported overall within the EU, there are certain indications that **not all sectors in all Member States expect to be totally ready** and fully compliant in time. A major element in this is the **lack of available** (verifiable) **information** on the situation particularly in relation to the potential spill-over effects between Member States.

Every sector consistently reports that, in particular, **smaller organisations continue to lag significantly behind large companies** in addressing the Y2K problem, and all organisations retain a **strong dependency upon their IT system suppliers to provide an accurate disclosure of the compliance of their products and to deliver timely compliant upgrades**.

A major consideration is the need to give recognition to the important role played by regulatory authorities, as well as by organisations such as insurance companies. In the coming months, these **regulators** and insurance companies **will have to take decisions concerning whether to continue to license or certify certain companies to continue to operate**, and whether to provide continued insurance cover. Due to the key role of infrastructures, such decisions may have an impact which goes well beyond the particular company or an individual Member State. Issues of potential civil liability, also in a cross-border context, will need to be carefully examined.

So there is a need for greater co-operation between regulators to share the strategies, criteria and information on which they will base such decisions. It is also necessary however, for governments to back the decisions of the regulators.

With regard to the situation beyond the Union's external borders, ***the assessment of possible safety issues in nuclear installations (power plants and other nuclear facilities) and power grids in Eastern Europe and the former Soviet Union is of perhaps the most concern and should continue to be addressed without delay.***

There is a lack of available (verifiable) information about the state of preparedness of key EU infrastructures On the basis of this information it is difficult to make a clear assessment. There are also certain indications that not all sectors in all Member States may be fully ready and compliant in time. These are reasons for concern.

Political action is necessary

The interdependencies between sectors, the importance of essential services, especially energy the dependency on external EU supplies in sectors such as oil, gas and the need to ensure access to emergency telecommunications services, **require political attention of Member States** in order to minimise remaining risks and to focus on contingency planning.

Given that **disruptions to certain crucial infrastructure services and supplies may possibly occur**, and indeed that the risk of accidents having unexpected spill-over, domino effects also exists, **EU Member States must ensure that effective contingency plans are prepared or, in case of existing ones, reviewed and made fully operational in time**. Such contingency planning should be based on co-operation between the private and public sectors; cater for a wide range of possible scenarios; and should take full account of trans-national dependencies. Since many existing plans will assume that other infrastructures continue to operate normally, Y2K contingency plans will now also have to be verified against various scenarios in which other infrastructures may no longer be fully functional.

An important element in addressing the Y2K issue is the **need to ensure that adequate resources are devoted to its resolution by all both the public and the private sectors.** The may mean the need to establish priorities and, if needed, temporarily move resources from other projects and activities.

Given this situation, there is a clear political responsibility of the public institutions at all levels to intensify work on the Y2K issue, to reassess the weight of its impact upon those areas under their responsibility, and to pay particular attention to transborder effects and contingency planning.

On the basis of the above analysis, the Commission draws the following conclusions to intensify near-term work on the "Millenium Bug":

Conclusions:

⇨ Member States should continue to make available the necessary information to the public, to other EU governments and neighbouring countries on the state of preparedness of their vital infrastructures and services in the areas of energy, water, food and pharmaceutical supply, healthcare, telecommunications, finance, transport, and social security.

They should ensure that regulators and government authorities have the necessary resources to carry out auditing tasks and take the appropriate measures in cases where safety and/or public health concerns arise, supported by any appropriate policy action.

Regulators, and public authorities in the Member States, in cooperation with industry, should finalise contingency and safety plans, verify their functioning in relation to infrastructure dependencies and their effective cross-border operations and, where necessary, reinforce co-ordination.

⇨ Work should intensify at all levels, both in the private and public sectors, including on-going work being undertaken in the Council with the assistance of the Commission, to share information and to coordinate actions, in particular with regard to the cross-border aspects of contingency and emergency planning, including the response during the critical period.

⇨ The situation in relation to nuclear installations, in particular powerplants as well as powergrids, in the CEEC and NIS countries and the possible impact on the EU is of concern.

The Commission suggests that Member States continue to make available technical expertise, in particular:

- to the IAEA to assist countries in the auditing of their power plants,
- and to support these countries in the assessment of their power grids and in developing and implementing appropriate contingency plans.

The state of preparedness in specific infrastructure sectors.

Energy sectors in general

In the energy sectors, utility companies have generally been working on the problem for a number of years now and within the EU, they are confident that their systems will be mostly Y2K compliant. However, many reports still cite residual problems, delays, and uncertainties, especially with respect to the continuity of external supplies.

Electricity

Electricity is a backbone of all essential services. The quality of supply must not be reduced, nor should there be any compromise on safety. The 1 January 2000 will occur on a Saturday in a holiday period, where demand is likely to be significantly below maximum levels. **Nevertheless, there may be failures**, likely to be localised, **which in the middle of winter could have serious consequences** for the areas concerned. Utilities must therefore undertake all possible preventative and mitigating measures, particularly adequate contingency planning.

An additional consideration is the so-called "grid problem", which is of particular concern in CEEC and the NIS. The unplanned shutdown of several power stations (nuclear or thermal), shutdown of an important user, or problems with grid control equipment could in turn induce problems in power plants (nuclear or thermal).

With respect to cross border flows, European utilities are adopting a policy of increasing spinning reserves and retaining their connecting links in operation, but reducing flows to a minimum, thus fulfilling contractual obligations and also permitting mutual assistance to be given if needed.

Gas

The gas supply organisations have been working for some time on making their systems compliant. Compared to electricity however, the cross border effect for natural gas is much more significant. Whereas a relatively small proportion of electricity flows across national borders – apart from one or two countries – **43% of natural gas originates from outside the EU**. Moreover, 22% of the total energy demand is covered by gas. These external supplies are obtained primarily from Russia, Algeria and Norway, and the gas must flow across several countries through major pipelines to reach the various destinations.

To assure uninterrupted and safe gas delivery during the millennium transition, even in the unlikely situation that something goes wrong either internally or externally, contingency plans are being put in place. Remote-controlled stations can be operated manually and additional stand-by personnel will be available. Alternative back-up telecommunication lines and private radio networks are being established and there is an advance agreement with partners to maintain supply and to provide mu-

tual assistance between gas companies. Furthermore, gas storage is available in every country to cover the normal consumption during a certain period of time.

Nevertheless, **there may be a need to strengthen co-ordination at EU level in order to support national contingency planning activities** should an interruptions occur to the normal supply of gas from a particular foreign country.

Oil and coal

Oil can be readily stored, thus those who are dependent on this fuel for heating can have stocks in place. Moreover, for the oil supply industry as a whole, substantial oil stocks should exist, to meet the levels required under EU legislation for general supply security reasons (90 days consumption required to be held by the industry or designated agencies for each Member State).

Nevertheless, **the dependence on non-EU oil supplies, at nearly 80%, is high**, and as with natural gas, it is not possible to be certain of the effect of Y2K on external producer countries. Member States should therefore ensure that contingency plans are able to deal with any temporary disruption in supplies, and confirm that measures have been taken for the key installations within their territory.

Furthermore, it is possible that there might be a surge in demand by customers for oil products such as gasoline or heating oil as the critical period is approached and reserve stocks are built up. Suppliers may need to prepare for this, as well as for possible disruptions to the supply chain itself, by making use of their own storage and flexibility measures. Those installing stand-by generators will also need to have adequate fuel stocks in place.

The **coal sector is perhaps the energy form of least general concern** with respect to the Y2K problem. In part, this is because indigenous production of coal in the EU has declined considerably. It is clear however that the companies involved must take measures to prevent disruption to their production. Likewise, consumption is rather concentrated, and is mainly accounted for by power generation, steel and other industry, though these users too will need to take measures to assure their supplies and to hold an appropriate level of stocks.

Nuclear safety

There are two main sources of concern related to nuclear power plants. First, there is a risk that on-site systems may fail. Although it is claimed that only limited use is made of digital logic in safety-related systems, there is a possible risk that multiple failures in other systems, while not intrinsically unsafe in themselves, could overload nuclear power plant operators and induce errors. Second, there are concerns that any unplanned shutdown of several power stations (nuclear or thermal), or any shutdown of an important user or problems with grid control equipment could provoke grid problems, which in turn could induce problems in power plants (nuclear or thermal).

Inside the European Union

Member States with operating nuclear power plants have action plans to address the issue. These action plans differ in detail but each requires the operator to identify

systems that might be affected, to rank them by nuclear safety significance, to test each in turn and to address any failures. Regulatory authorities are reviewing these action plans and are monitoring their execution. Most reactor operators report they will be Y2K ready by mid-1999. It will be up to Member States and their regulatory authorities to ensure that this is indeed the case and provide the necessary information, and confidence, to the public.

Outside the European Union

Regarding CEEC and NIS, the general view is that there is a lack of confidence that the two main sources of concern have been appropriately checked (including contingency plans). This *concerns primarily the 50 nuclear power plants* but also research facilities and other nuclear facilities. Despite the claimed, limited use of digital logic in safety related systems in eastern European nuclear power plants, there are Y2K problems with some systems. Special attention should be paid to newer equipment installed recently.

The International Atomic Energy Agency (IAEA) is addressing the Y2K problem on nuclear power plant sites. The IAEA will organise assessments over the next two to three months, followed by a phase of contingency planning (Chernobyl has been assessed). Its immediate needs relate to the assessment phase, to be implemented by small teams of Western experts, in co-operation with local operators. **The IAEA has already requested the Commission support for inspection missions to three nuclear power plants** (Kozloduy – Bulgaria, Zaporozhe – Ukraine, a still to be identified plant in Russia), but is expected to request further assistance in the next months. The IAEA assessment teams will report back and a clearer picture of the needs will begin to emerge by July. Given this late date, it is unlikely that requests for replacement, compliant equipment can be addressed by the end of the year. Therefore the focus must be on contingency planning.

The Commission services are discussing the practical modalities of this support with the IAEA and the World Association of Nuclear Operators (WANO). The Commission has asked WANO to undertake the IAEA assessment at all the sites where it is needed; as such a scheme would minimise the administrative burden, maximise the use of expertise, and ensure the comparability of results and the contingencies to be proposed.

The International Science and Technology Centre (ISTC) in Moscow established a special fund (1.35 M$ currently pledged) to help Russian and NIS institutions solve Y2K issues, using staff of former weapon research institutes. ISTC funds will support co-ordination of the definition of methodologies, assist Minatom and other institutions in projects to implement practical Y2K solutions, identify international collaboration and assist in provision of specific international expertise. **However, no guarantees can be given that assessments are performed in time, nor that contingency plans will be ready.**

As far as the Commission is aware, **at present no international organisation is able to co-ordinate an assessment of the risk presented by "grid failure" in the CEEC or NIS**. In view of the potential risk to nuclear power plants, to imports from NIS (e.g. gas) and the ***general risk to citizens in the CEEC/NIS, urgent attention***

needs to be paid to this issue. Further funds need to be made available immediately for such an assessment.

Water supply and wastewater treatment

Many other sectors rely on water supply. Although activities in this area have generally had a late start, the water supply and wastewater treatment sectors in the EU have recognised the threat posed by the millennium bug and progress is reported.

With respect to wastewater, most countries report that separate ministry and local government bodies are responsible. Each is therefore responsible for its own millennium projects, including contingency planning. This sector is dependent upon energy for its operation. Problems might arise due to temporary breakdowns of wastewater pumping stations and due to a reduction of the efficiency of treatment plants. The first could cause local problems with wastewater disposal, the second also could lead to an increase in to water pollution downstream of the wastewater discharge. Limited services can be provided when normal resources are unavailable. The sector is making progress, although supplier dependencies are of concern because the lack of information on certain technical installations.

The **main risk identified in the sector is the possibility of pollution of surface waters used for drinking water abstraction intake** from major rivers as a consequence of the millennium problem.

Telecommunications

The overall general dependency on telecommunications networks is a simple, if obvious, part of the shift to the information age. All sectors need to communicate to function.

An important difference between the telecommunications sector and other sectors is that while some expect lower than normal demands, the telecommunications sector will probably be overloaded by people calling to wish each other a happy millennium. Network saturation has been reached in the past in similar circumstances. Moreover, this naturally occurring demand is likely to be aggravated by an increase in the number of faults and accidents occurring in other sectors which will require use of the telecommunication networks in seeking to obtain remedial action. The strong possibilities of network saturation gives rise to the **clear need to ensure a continuing priority to emergency and other essential services**.

There is no reasonable expectation that the infrastructure will be enhanced to deal with it. This is a transient problem, independent from the IT effects of the date change, which can be managed by various techniques. There is a need for detailed discussions to take place in order to ensure that emergency services can be reached during the peak period and that network saturation is mitigated for this purpose.

Like electricity, telecommunications is a real time service, which cannot be stored. Unlike electricity, spare capacity in one place cannot necessarily be transferred to assist if there is congestion elsewhere.

A further characteristic of telecommunications networks, one that they share with other sectors, is the limited possibility to carry out real-life testing. A service that is relied upon every minute of every day cannot be switched off to allow testing.

The main telecommunication networks are dependent on electricity. Short breaks in supply should be handled by the generators and batteries already in place.

Substantial activities are ongoing at international and national level to ensure that networks are prepared. However, it is considered that operators outside the EU may not be equally well prepared and that **disruption to the international telephone and fax networks cannot be excluded**. Recognising the scale of the threat posed by potential Year 2000 computer failures and the critical role played by the globally deployed telecommunications networks, the International Telecommunication Union (ITU) established a Year 2000 Task Force in March 1998. Activities include a review of expected states of readiness of all major operators world wide, an extensive programme of inter-regional testing, the sharing of information and the promotion of contingency planning.

Important work is still required in this area, as other sectors rely upon the continued availability of telecommunications for their own contingency plans. Telecommunications is the prime tool for reporting outages or other issues which could have an impact on the economy as a whole.

Aviation

The parties involved in this sector - airlines, ATC service providers, airports, national regulators and certification bodies – report that they have reached an advanced stage in their preparations to ensure Y2K compliance. In particular, safety and security systems are being upgraded and tested in accordance with well-defined management plans; although commercial and facilitation applications, notably in airports, are not yet completely tested and full Y2K compliance will probably not be entirely guaranteed.

Although both regulatory authorities and industry (Eurocontrol, JAA) have expressed confidence with regard to the state of compliance, given the paramount importance of safety, contingency plans are being developed which would ensure safe operations even in a worst-case scenario. These will be based largely on well-established operational procedures, which are being reviewed to ensure their appropriateness to address Y2K issues. Whilst contingency plans will cover immediate safety concerns satisfactorily, the possibility of certain capacity constraints occurring during the immediate period following the changeover cannot be excluded.

The two most critical cross-sector dependencies are telecommunications and electricity. Contingency plans include the use of satellite phones and diesel generators, but these are emergency back-ups and not real solutions. Efforts for cross sector co-operation, carried out at local and national level, should be reinforced.

The overall preparations by Western European industry appear to be well advanced, but the risks associated with cross-border interactions with neighbouring regions of the European Union remain to be assessed more fully. Information on the weaker components of the air transport chain, including certain national regulators, is not yet forthcoming but should be provided through the report of the International Civil Aviation Organisation, due mid-1999. The aviation industry is being advised by regulators

that if they are not satisfied with Y2K compliance and they have safety concerns, action will be taken to withdraw operating authorisations.

Maritime transport

Although the potential of Y2K to create problems in the maritime sector may appear less significant than in aviation, many vessels carry cargoes that are essential for the economy, so any interruption in the logistic chain could have serious and widespread consequences. Furthermore, there are potential dangers to the environment with some cargoes, if safe handling can not be assured. Attention has been paid to safety critical functions both at sea and in ports. However, doubts remain about certain functions and the compliance of some ship owners, particularly those with so-called 'flags of convenience'.

There is a need to reach agreement between the different authorities on the question of how to handle suspected substandard ships during the changeover period. The work of the shipping and port associations has identified the need to allow all parties concerned to have the possibility to control ship movements, either by requiring vessels not to enter or leave ports, or for ship captains to decide to remain at sea if they suspect problems onshore.

EU maritime and port associations are continuing to urge members to adopt contingency plans: further efforts are needed to ensure full compliance.

Rail transport

There are a number of different IT systems used by railways in which problems of compliance could arise. Non-compliance is unlikely to compromise safety but could disrupt rail traffic or services to freight and passenger customers. Ensuring the compliance of the interconnections between the railways' IT systems is a particularly complex task. While components of this network have been checked, end-to-end tests have not been carried out.

Regulators are generally taking the leading role in the assessment of business continuity aspects, as well as safety aspects. Audits are being performed and the results kept under review. Risks are limited in this sector, primarily associated with the power supply and the international context. Minor and limited disturbance to local information systems for passengers cannot be excluded.

Finance sector

In the EU, as elsewhere, the financial sector is still generally considered to be the most advanced sector, although it is also dependent on other crucial infrastructures such as electricity and telecommunications.

As far as the internal preparation of financial institutions is concerned, certain EU countries noted that their financial organisations had tended to delay their year 2000 adaptation processes, due to the fact that the changeover to the euro was receiving high priority in the financial sector. However, this has had a generally positive result. Indeed, all institutions of the four financial services sectors (banking, insurance, se-

curities, payment systems) have undergone an exercise of parallel euro and Year 2000 adaptation projects.

The euro changeover has had another benefit, in that many of the contingency strategies for Y2K are being based upon the contingency measures adopted for the euro changeover. The successful experience of EU financial institutions in coping with the similar euro changeover challenge has generated confidence in the ability of companies to implement such changes successfully.

However, there is a tendency to underestimate risks not directly associated with information system failures (credit risks, liquidity problems, business-to-business risks, systemic disruptions, coverage of client Y2K risks, and litigation). Although these issues have been identified as potential problem sources, firms have concentrated on their internal adaptation programmes and may now lack the resources, time, or simply the ability to take appropriate measures in order to protect themselves against such risks.

Furthermore, the supply of information to the public by the financial sector and by public financial authorities could still be improved. Many companies have yet to adopt proactive strategies to disclose to the public their Year 2000 situation. These organisations may be underestimating the impact of their attitude, not only to the public but also to the potential impact on international financial markets as there is a risk of turmoil being generated by the erroneus or ill-informed opinion of certain international financial experts. If this were to persist, this lack of attention could impair the competitive position of the European financial sector, in spite of the substantial progress which has indeed been made.

Food and pharmaceutical supply chains

The supply chains which are of greatest importance at a national level are the food and pharmaceutical supply chains. Within the EU, the major food manufacturers and retailers are collaborating to share information and experience, and to develop practical business continuity plans. It is imperative that this sector continues to co-operate, particularly in forecasting customer behaviour and predicting demand well in advance, thus ensuring that supply will be able to meet possible unusual surges in demand towards the end of 1999.

There is a similar rationale for the need to take action in the pharmaceutical sector. The European pharmaceutical industry must work together with hospitals to identify their requirements for medicinal products during the critical period, and also to inform the public of their progress and plans. Between the US and Canada, there is a mutual agreement that their hospitals will not stockpile medicines. Once again, an additional concern is the external situation, since many of the active drug substances used to manufacture prescription generic pharmaceuticals originate outside the EU.

Healthcare

Healthcare is generally dealt with at local level by individual hospitals in Member States, although some countries have established national co-ordination mechanisms to share information between hospitals. There is no international body addressing the sector and no exchange of information taking place between countries. The main problem identified in this sector is the difficulty in obtaining information from suppliers on the compliance of products, especially electronic machines for medical and health purposes containing embedded chips, in use within hospitals. This is an area where Member States, particularly at local level, need to be vigilant.

Social welfare payments and tax collection

For the public sector, key services which have to function are welfare payments and tax collection. Most Member States report that they are devoting particular attention to the IT systems in these areas. It may be necessary to consider the availability of temporary, emergency cash pay-out systems to ensure that citizens continue to receive welfare payments.

ISSN 0254-1475

COM(1999) 275 final

DOCUMENTS

EN **15 16 01 10**

Catalogue number : CB-CO-99-282-EN-C

Office for Official Publications of the European Communities
L-2985 Luxembourg