1998/45. Suggested guidelines for addressing the year 2000 problem of computers

The Economic and Social Council,

Recalling General Assembly resolution 52/233 of 26 June 1998 on the global implications of the year 2000 date conversion problem of computers, in which the Assembly, *inter alia*, called upon the Economic and Social Council to prepare guidelines on which Member States would be able to draw in addressing the diverse aspects of this problem,

Recognizing the serious risks posed by the year 2000 problem and the urgent need for Member States and all parts of the United Nations system to achieve compliance well in advance of the inflexible date of 31 December 1999,

1. *Adopts* the suggested guidelines for addressing the year 2000 problem of computers contained in the annex to the present resolution;

2. *Requests* the Secretary-General to ensure broad dissemination of the suggested guidelines for maximum utilization by Member States and those areas of the United Nations system that are not yet year 2000 compliant, as a matter of urgency.

47th plenary meeting
31 July 1998

ANNEX

Suggested guidelines for addressing the year 2000 problem of computers

The objective of the present guidelines is to raise the awareness of Governments on the year 2000 problem and compile a general list of issues that should be considered in this context. The problem stems from the fact that many hardware and software systems use only the last two digits of the four-digit designation of a given year to identify that year. Hence, if not converted by the target date, 31 December 1999, those systems will recognize "00" not as the year 2000 but instead as the year 1900. Electronic systems that are not year 2000 compliant and involve processes based on dates will either shut down, produce meaningless and misleading results or revert to some other date, as a result of which whole sectors of the economy and critical government operations could experience significant disruptions.

Although there is an abundance of material available on the Internet from expert groups and government and private institutions warning about the impact of the date issue, it is felt that there is still a need to stress the complexity of the problem, which could affect not only businesses and Governments but also international cooperation. If one partner in a private or intergovernmental network is not year 2000 compliant, this could create a domino effect, causing the whole network of cooperation to break down and affecting even compliant segments. There is also a misconception that the problem is limited to computer systems. In fact, all equipment configurations with embedded systems that use code or chips and involve the handling of dates could be affected. Misunderstanding of the year 2000 problem as being a problem of individual computer systems has led to the belief that the finding of solutions can be left to technical experts. However, recognition of the fact that the millennium bug affects a wide range of different systems and that a domino effect is possible has led to the understanding of the year 2000 problem as being also a management problem.

This brief note attempts to summarize the issues involved and provide general guidelines for attacking the problem; for more detailed information, readers are referred to the Internet and the other sources of information mentioned above. Although the four-step procedure outlined below is geared to government institutions, most of it applies equally to the private sector.

1. *Problem awareness*

   - Governments and international organizations, at the highest level, should announce their commitment to meeting the year 2000 challenge. Progress should be publicly reported at regular intervals;
   - A year 2000 awareness campaign should be initiated and directed at target groups, such as small businesses and local government agencies, that may still not be aware of the issue and its complexities;
   - A comprehensive year 2000 strategy should be developed that would allow Governments to address the problem in a coordinated manner. The strategic recommendations should be translated into tactical objectives by local governments or executing agents;
   - Cooperation between Governments and the private sector should be initiated at all levels of government, including the national and international levels.

2. *Problem assessment*

   - A management structure should be put in place that assigns clear responsibility and authority for addressing the various aspects of the problem;
   - Year 2000 compliance should be clearly defined in operational terms and standards should be established for determining what constitutes compliance. For critical systems, a formal certification procedure should be considered;
   - Some consensus regarding the order of criticality of processes should be reached. Criteria to be considered are: preventing loss of life, allowing

effective government, maintaining civil order, avoiding large-scale hardship, allowing continuation of commercial activities, preventing environmental damage, and so forth;

- Sectors of the infrastructure and systems of national importance for which compliance must be assured should be identified. The list should include but should not be limited to transport and communication, utilities, finance, national security, public health, nuclear facilities and international relations;

- Each organization responsible for providing critical services should be encouraged or required to develop a plan to solve its year 2000 problems. The plan should outline steps to be taken in systems assessment, repair, testing, implementation and coordination with other entities;

- For areas that are not of primary national importance, a risk analysis should be carried out to establish an order of priority for ensuring compliance. It is now recognized that 100 per cent compliance will be difficult to achieve. For low-risk areas where non-compliance will have little impact, action could be delayed;

- To avoid a domino effect, interdependencies between systems of low priority and areas of national importance must be identified;

- The interface between national systems and the systems of other Governments should be defined. Particular attention should also be given to private-sector service providers, for example, in the areas of communication, air traffic control and power supply, who operate on a regional or global level but are an integral part of the national infrastructure;

- Mechanisms for disseminating candid information about the status of remediation should be established;

- Questions regarding public and private sector liability for damages resulting from non-compliance and warranty issues should be investigated.

3. *Problem solution*

- Validation strategies and testing procedures for all converted or replaced systems and their components should be established;

- A manpower analysis should be carried out to determine the human resources required for the conversion. Many countries, especially developing countries, are already experiencing a shortage of skilled information technology workers. This problem will be aggravated by the year 2000 issue. Developing countries will be particularly vulnerable;

- Budgetary provisions must be made to secure funds for new hardware, conversion software, human resources and related costs. Further, the financial responsibility for the cost of conversion must be determined. Some countries may consider funding by international organizations, especially the World Bank, which has grant loan funds available;

- Suppliers and designers of systems should be identified and integrated into the validation and testing process, whenever possible;

- As regards the application of the validation and testing process established earlier, systems will be certified or steps to convert systems will be taken according to their priority. Since problems and their solutions may be similar across applications and processes, a mechanism for the exchange of information and the consolidation of activities should be established at the national and international levels.

4. *Contingency planning*

- Governments should establish general contingency plans for all systems and activities of national importance and the systems that support them for continuity of operations. Back-up arrangements should be made at the national and international levels;

- A hotline should be established so that the public can report possible millennium-related problems and obtain assistance in case of emergencies;

- The disaster recovery plans of all systems should be reviewed and updated to avoid loss of data and ensure the resumption of operation as soon as possible;

- In case year 2000 compliance cannot be achieved before 31 December 1999, some critical systems may have to be temporarily decommissioned and replaced by back-up processes. Planning for the establishment of back-up processes for critical infrastructure systems should start immediately. It is important to determine how far in advance such plans will need to be implemented so as to be effective in the event that the deadline cannot be met.