partnerships with each other and with representatives from business, labor, academia, and the public.

1. Privacy Protection

By bringing news and information to people on a global basis, and thereby allowing them to communicate more freely with each other, communications technologies serve a democratizing function. These same technologies also permit both governments and the private sector to transmit, process, and store vast amounts of information about individuals. While these capabilities are increasingly essential for governments to function effectively and for businesses to operate efficiently, questions continue to grow about an individual's right to privacy and the accompanying responsibilities of holders and transmitters of this information to safeguard this right.

In many nations, the past two decades have seen the primary gatherers and users of personal data shift from government entities to private sector firms. In the 1970's and 1980's, businesses were quick to exploit the explosive growth in low cost, high performance computers, adapting this technology to a wide range of economic, financial, and marketing applications. As electronic commerce spread during the 1980's, there was growing recognition that the electronic transfer of data across national boundaries required an international consensus on

individual privacy protection. In 1980, the OECD developed and adopted a set of voluntary privacy guidelines that were accepted by its 24 member countries. In 1981, the Council of Europe, whose membership consists of the European Union Member States and other European countries, adopted "fair information practices" similar to those of the OECD to regulate the collection, storage, and automated processing of personal data, and transborder data flow. Both the OECD and Council of Europe privacy guidelines, which generally recognize that the free flow of information is critical to transborder economic activity. provide a framework for domestic legislation that has been used by both member and non-member nations. They also recognize diverse means of protecting information privacy, including self-regulation and industry codes of conduct. The North American Free Trade Agreement (NAFTA) and the General Agreement on Trade in Services (GATS) Annex on Telecommunications also contain provisions that recognize national privacy protection regulations.

The United States and other countries around the world are re-examining

existing privacy policies to ensure that they apply comprehensively to the transfer of personal data over global networks. A balanced privacy policypreserving the individual's right to privacy while maintaining the free flow of information across national borders is important to the development of global networks and services. Working together, nations should ensure that the transport of personal data adequately takes into account the following agreedupon international privacy principles:

 Personal data should be collected only for specified, legitimate purposes;

• The dissemination, sharing, and reuse of information should be compatible with the purposes for which it was originally collected;

 Personal data should be accurate, relevant, and up-to-date;

 Individuals should be informed how personal data will be used and should be allowed to examine and correct this information; and

 Transmission of personal data should not be unduly restricted or subject to burdensome authorization procedures.

Recommended Action

In order to foster consumer confidence in the GII and to encourage the growth of interconnected global networks, users must feel that they are afforded adequate privacy protection. To this end, the United States will join with other governments to:

 Identify key privacy issues that need to be addressed in relation to the development of national and global information infrastructures;

· Work with both the public and private sectors to achieve consensus on a set of fair information principles for the collection, transfer, storage, and subsequent use of data over national and global information infrastructures;

 Ensure that privacy protection does not unduly impede the free flow of information across national borders;

· Share information on new privacy protection policy developments and on new technologies and standards for privacy protection; and

 Encourage the use of voluntary guidelines developed by international bodies, such as the OECD, as the best means of ensuring the protection of privacy on an international basis.

2. Security and Reliability

A network as vast and complex as the GII will pose difficult security challenges for all nations. The same modern technology that makes communication faster and easier also makes communications systems vulnerable to ever greater security risks.

These risks are not new-most are wellknown among security managers. What is new is that these risks are much more widespread, are potentially much more serious, and affect a population of users who do not have the information or training to deal with them.

The anonymous and impersonal nature of computer crime, for example, makes this problem particularly unsettling, for legal systems depend upon their ability to identify the malfeasors. Yet serious violation of privacy or property rights can be accomplished by destruction or alteration of information by anonymous individuals in remote locations, with not a fingerprint in sight. The technical challenges of protecting the privacy and integrity of information stored in computer systems are even greater than those that apply to information transmitted by telephone. And as was true with the telephone, legal as well as technological solutions are needed.

Security includes the integrity confidentiality, and reliability of the networks and of the information they carry. If users do not believe that an information infrastructure is a trustworthy, reliable system, they will be reluctant to use it, thereby diminishing its value. To gain maximum benefit from global networks, users must be confident that the messages they receive are authentic, that sensitive information is available only for authorized use, and that unauthorized users cannot access, alter,

or destroy information.

In addition to protecting the security of information that is transported over the GII, governments and industry must guarantee the reliability of the network itself. In the event of breakage or service interruption, network operators must work quickly and cooperatively to repair damage and provide backup systems to minimize the duration of any such interruptions. To have a truly global infrastructure, greater emphasis must be placed on resolving reliability concerns, including such issues as network performance, network connections and interoperability, the development of new technology, and regional and demographic differences in reliability.

Recommended Action

To promote the development of a secure and reliable GII, the United States will join with other countries to:

- · Work collectively to increase the reliability and security of national and international information infrastructures:
- · Initiate a broad international dialogue among users, providers, and all