OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: TOWARDS A CULTURE OF SECURITY

QUESTIONS AND ANSWERS

Q1. What is the nature of the 2002 Security Guidelines?

They are non-binding Guidelines and, unlike conventions, governments are not "legally bound" by these Guidelines. The nine principles set out in the Guidelines reflect the agreed position of OECD countries and have the support of the international business community and consumer protection organisations. Member governments are also committed to implementing the Guidelines.

The key aim of the 2002 Security Guidelines is to provide governments, business and individual users with guidance for protecting the security of information systems and networks in a climate of increasing potential threat to these systems, and to provide a common international approach to creating a worldwide "culture of security".

Q2. When will the 2002 Security Guidelines go into effect?

The 2002 Security Guidelines were adopted by the OECD Council on 25 July 2002 and are currently in effect. The OECD Press Release of 7 August 2002 launches the Security Guidelines Awareness Campaign.

The implementation of these Guidelines has already commenced in capitals around the world. The Guidelines are currently available in English, French and Spanish, and most other member countries are in the process of translating the Guidelines at this time.

Q3. Why do we need the 2002 Security Guidelines?

Given the ubiquitous role of the Internet and increasing potential threats and vulnerabilities to our new "networked world" governments and business are calling for a culture of security for all "participants" to ensure the security of our national and international information systems and networks. .

Q4. Who is concerned?

Every "participant" (governments, businesses, other organisations and individual users who develop, own, provide, manage service and use information systems and networks) connected to the networked world is concerned with the security of information systems and networks. The numbers stretch to more than 200 million Internet subscribers and an estimated 500 million users in OECD member countries alone. The implementation of these Guidelines is relevant, however, to all participants in all nations and the OECD will co-operate closely with its international partners to implement these Guidelines. Each participant is expected to play his/her own role, too, in protecting the security of information systems and networks. Security is only as good as the weakest link in the system.

Q5. What should governments do?

Governments are expected to promote a culture of security through education, training and awareness-raising activities. Where necessary, governments are encouraged to establish a new policy or amend existing policy with regard to the protection of information systems and networks, according to the nine principles included in the 2002 Security Guidelines .

As government has the largest procurement of security systems, governments are expected to attach great importance to the protection of the security of these systems and to set a good example for the rest of the world's participants.

Q6. How can business contribute?

Suppliers of services and products should bring to market secure services and products. Business plays an important role in standards making in the industry and are expected to continue to treat security as one of its highest priorities in design and implementation of new and existing systems. Business is also expected to supply timely and pertinent security information, such as "security-hole" patches and virus protection updates to users.

As business is one of the greatest users of security systems, business is expected to continue to attach great importance to the protection of the security of these systems by informing their employees of security policies and empowering them to implement them.

Q7. What are individual users expected to do?

First of all, individual users need to be aware of potential security risks and the available safeguards for their systems. With this knowledge, they also need to be responsible for maintaining the security of their systems according to their roles. For example, they need to update their systems and software regularly so that known security holes are eliminated from their systems. They also need to understand and implement common security practices, such as shutting down their computers when leaving the offices and homes, not opening unidentified e-mails, not sharing passwords, introducing anti-virus software and not opening unknown executable files.

Individual users need to be instructed and supported by both government and business (suppliers), where appropriate.

Q8. What is a "culture of security"?

Every participant should be aware, responsible and take the appropriate actions to ensure the security of their information systems and networks. The actions should be consistent with the values of a democratic society, such as the need for an open and free flow of information and basic concerns for personal privacy. The principles in the 2002 Security Guidelines provide the foundation for work towards creating a culture of security for all participants.

Q9. How does the OECD plan to implement the 2002 Security Guidelines?

The first step is to disseminate the 2002 Security Guidelines and to encourage all participants to read, understand and implement the Guidelines according to their roles in the networked world. The OECD is inviting its partners (member and non-member governments, business, consumer organisations and other organisations) to work on their own implementation plans of the Guidelines. Actions that should be taken by each sector will certainly differ. Comprehensive and well-planned education and public campaigns may be necessary. Best practices and bench marking may be used for information exchanges. The implementation measures will be reviewed regularly.

Q10. Does the release of the 2002 Security Guidelines relate to the September 11 incidents and if so, how?

After September 11, 2001, international attention has focused heavily on various dimensions of security such as security for nuclear power plants, shopping malls, sports stadiums, and airports, to name a few. Security for information systems and networks, too, have received significant attention, including the various dimensions of computer and network security and vulnerability (*e.g.* critical infrastructures such as banking, energy, transportation systems and networks). Stronger information security was identified to be increasingly critical to society today, whose functions are highly dependent on the well-being of information systems and networks.

Q11. What do business and consumer-protection organisations think of the 2002 Security Guidelines?

The OECD has worked very closely from beginning to end with business and consumer protection organisations on the drafting of the 2002 Security Guidelines. The OECD has received strong support for these Guidelines and their implementation from both our business and consumer protection partners.

Q12. How can the public obtain a copy of the 2002 Security Guidelines?

The 2002 Security Guidelines will be on sale in all OECD Sales Outlets in early September 2002. The Guidelines are also available free online at **www.oecd.org/sti/security-privacy** in English, French and Spanish. Governments and many organisations will also be making the Guidelines and other security material available in their capitals in the near future.