OECD guidelines seek "culture of security"

By Eugene Oscapella

IN THE LIGHT OF LAST YEAR'S September 11th attacks in the US, the Paris-based Organisation for Economic Cooperation and Development (OECD) has revised its security guidelines.

On July 25th, the *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* were adopted as a recommendation of the OECD Council. They replace the previous OECD security guidelines that were created in 1992.

The guidelines' preface explains that the use of information systems and networks, and the entire information technology environment, has changed dramatically since the original guidelines. "These continuing changes offer significant advantages, but also require a much greater emphasis on security by governments, businesses, other organisations and individual users who develop, own, provide, manage, service and use information systems and networks ('participants')."

The guidelines refer to the need to develop a "culture of security" through greater awareness and understanding of the issues. An OECD press release refers to the need for new guidelines in the wake of last year's September 11th attacks in the US. The goal was to counter cyber-terrorism, computer viruses, hacking and other threats.

The guidelines are non-binding, although the press release notes that they are the product of a consensus between OECD governments resulting from discussions that also included representatives from the IT industry, business users and civil society. OECD governments and other participants will, therefore, draw on them to establish policies, measures, and training programmes for online security. The Guidelines consist of nine complementary principles, which are to be read as a whole:

1. **Awareness –** Participants should be aware of the need for security of information security systems and networks, and what they can do to enhance security.

2. **Responsibility –** All participants are responsible for the security of information systems and networks.

3. **Response –** Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents.

4. **Ethics –** Participants should respect the legitimate interests of others.

5. **Democracy –** Security of information systems and networks should be compatible with the essential values of a democratic society.

6. **Risk assessment –** Participants should conduct risk assessments.

7. **Security design and implementation –** Participants should incorporate security as an essential element of information systems and networks.

8. **Security management –** Participants should adopt a comprehensive approach to security management.

9. **Reassessment –** Participants should review and reassess security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

To implement the new guidelines, the OECD Council recommended several measures:

- Establishing new, or amending existing, policies, practices, measures and procedures to reflect and take into account the guidelines by adopting and promoting a culture of security as set out in the guidelines.

- Consulting and cooperating at national and international levels to implement the guidelines.

- Disseminating the guidelines throughout the public and private sectors and encouraging all the parties concerned to take necessary steps to implement the guidelines.

- Making the guidelines available to non-OECD member countries in a timely and appropriate manner.

- Reviewing the guidelines every five years in order to foster international cooperation on issues relating to the security of information systems and networks.

For further information visit: www.oecd.org/pdf/M00033000/M0033182.pdf; www.oecd.org/EN/document/0,,EN-document