ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

OECD OCDE

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE, ET DE L'INDUSTRIE
DIRECTORATE FOR SCIENCE, TECHNOLOGY, AND INDUSTRY

Markus Kummer
Executive Co-ordinator, UN WGIG
Palais des Nations, CH-1211 Geneva

22 March 2006

Dear Markus,

The OECD welcomes the establishment of the Internet Governance Forum (IGF) stemming from the World Summit on the Information Society (WSIS).

The OECD has been working for many years on a range of policy issues associated with the information society. These include infrastructure and services, consumer protection, privacy and security, through to broader issues surrounding ICT and economic growth. We view the IGF as an opportunity to further understanding in these areas and build international consensus, among all stakeholders, on effective ways forward.

With this in mind we also welcome the multi-stakeholder nature of the IGF. In our experience, such an approach is essential in dealing with the challenges facing the Internet, as well as taking advantage of the opportunities it presents to further economic and social development. By way of example, the OECD has a multi-stakeholder Task Force on combating Spam which has recently completed its work. The Task Force, after two years of work, will shortly issue a final report as well as a toolkit of various ways to effectively combat Spam.

More broadly, we have attached a brief summary of work undertaken by the OECD, in recent years, on issues highlighted in the IGF Secretariat's synthesis.[1] We believe we could make a significant contribution to the IGF under all these items. Notwithstanding this, there was a clear consensus, at the first consultation meeting (16-17 February 2006), that the IGF needed to select priorities and achieve focused outcomes from its first meeting.

We believe priority should be given to issues where the IGF has the greatest chance of success, in terms of building international understanding, and which further the goals of WSIS in terms of developing the information society.

Given the potential for a multi-stakeholder IGF approach to make a difference to the lives of everyday Internet users, and the timeliness of the work of the Spam Task Force using this approach, we would propose Spam as a leading issue to be addressed at the first IGF.

We stand ready to contribute on any of the other issues chosen by the IGF within our competence, from existing or ongoing work, which further the development of the information society.

The OECD looks forward to participating in further consultations on the convening of the IGF, to be held at the United Nations in Geneva on 19 May 2006, and as an observer at the meeting of the IGF Advisory Group on 22 - 23 May 2006.

Yours sincerely,

John Dryden

Deputy Director
Science, Technology and Industry Directorate
OECD

[1] http://www.intgovforum.org/brief.htm

## OECD work relevant to the IGF

Following the first Consultation Meeting on Convening the IGF, the IGF Secretariat posted a short synthesis of proposed topics (www.intgovforum.org/brief.htm). The following presents a brief and non-exhaustive summary of OECD work relevant to the IGF under some of the topics identified by the IGF Secretariat.[2]

### *A. Spam*

The *OECD Task Force on Spam* (2004) was set up to bring together policy-makers and industry experts to develop a framework aimed at tackling the problem of spam using a broad multi-disciplinary range of solutions. The Task Force has launched the Anti-Spam "Toolkit" (www.oecd-antispam.org) as an instrument to help governments, regulators and industry players orient their policies relating to spam solutions, support the development of national anti-spam strategies and improve cross-border co-operation between enforcement agencies. The Toolkit also includes a series of Best Practices developed by the private sector in its annexes, and will be completed by an OECD Council Recommendation on cross-border co-operation in the enforcement of laws against spam. The Toolkit is currently being finalised and will be publicly available by mid-April 2006.

### *C. Cybercrime*

Although the OECD does not directly work on cybercrime per say, several work threads cited in this summary contain relevant advice on policies and measures to address internal and external threats such as cyber-terrorism, computer viruses or hacking, in particular:

- The *Council Recommendation on cross-border co-operation in the enforcement of laws against spam* (2006).
- The OECD's *Scoping Study on the Measurement of Trust in the Online Environment* (2005) reviewed data available from official, semi-official and private sources on security, cybercrime and trust.
- The *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, (2003).
- The *OECD Guidelines for the Security of Information Systems and Networks* (2002), the report's promotion and the work on promoting a "Culture of Security", all of which are detailed in paragraph D.

### *D. Cybersecurity*

The OECD Working Party on Information Security and Privacy (WPISP, www.oecd.org/sti/security-privacy) promotes a global, coordinated policy approach to building trust and confidence in the use of ICTs, to ensure the security and reliability of systems and networks, services and transactions, as well as to protect privacy and personal data (see under item E). It develops international guidelines and tools for various facets of Information and Communication Technology policy, which are inherently global in nature and include:

- The *OECD Cryptography Guidelines* (1997) promote the use of cryptography to foster confidence in information and communication infrastructures, networks and systems, and their use.
- The *Use of Authentication Across Borders in OECD Countries* (2005) analyses the current cross-border uses of electronic authentication methods and methodologies in OECD member countries and the factors fostering or impeding the national use of authentication technologies and digital signatures.
- The *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002) aim to develop a "global culture of security" through advice on policies and measures to address internal and external threats such as cyber-terrorism, computer viruses or hacking in a globally interconnected society, while preserving important societal values such as privacy and individual freedom.

[2] An earlier summary of OECD work related to internet governance is available at www.oecd.org/internetgovernance

- The *OECD global "Culture of Security" Web site* collates national and international initiatives to implement the OECD Security Guidelines. It also serves as a portal for collective efforts the world over to develop a global "culture of security".
- The *Promotion of a Culture of Security in OECD Member Countries* (2005) is a major information resource on governments' effective efforts to foster a shift in culture as called for in the OECD Security Guidelines. It includes a detailed inventory of initiatives to implement the Guidelines in 18 OECD member countries and highlights main findings based on an analysis of common current trends in those countries and progress made since the adoption of the Guidelines.

***E. Online Privacy***

- The *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) represent an international consensus on basic principles to protect personal information and privacy on global networks.
- The *OECD Privacy Statement Generator* is an interactive tool available on the OECD Web site. It offers guidance on compliance with the Privacy Guidelines and helps organisations develop privacy policies and statements for display on their Web sites.
- The *OECD Privacy Online: Guidance on Policy and Practice* (2003) is based on the work achieved to fulfil the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks. Addressed to OECD member countries, business and other organisations, individual users and consumers, the report reflects the ministerial high-level objective to build bridges between different national approaches in order to ensure both effective protection of privacy and continued transborder flow of personal data on global networks. It highlights the importance of the OECD Privacy Guidelines in the development and implementation of a mix of solutions for ensuring global privacy (www.oecd.org/sti/security-privacy)

***G. International Interconnection Costs***

The work of the OECD Working Party on Communications and Information Services Policy (CISP) has long dealt with issues surrounding *interconnection* between communication networks.[3] In respect to the exchange of traffic between networks using the Internet protocol, the OECD has been active since the mid 1990s through a series of workshops (Dublin 1996, Osaka 1997, Venice 1999 and Berlin 2001) and reports (*Internet Traffic Exchange: Developments and Policy*, 1998, *Internet traffic exchange and the development of end-to-end international telecommunication competition*, 2002 and *Internet Traffic Exchange and Measurement of Growth,* Forthcoming 2006).

***H. Bridging the Digital Divide: Access and Policies***

OECD work in these areas include work on *Regulatory Reform as a Tool for Bridging the Digital Divide* (2005), on *Universal Access Funds with Minimum-Subsidy Auctions - Leveraging Telecommunications Policies for Pro-Poor Growth* (2004) and on *The Development of Broadband in Rural and Remote Areas* (2004). Further OECD reports on developments in communication infrastructure and services, including on regulatory reform aimed at developing access, are available at (www.oecd.org/sti/telecom).

Work has been undertaken on other aspects of the digital divide (see OECD Information Technology Outlook 2002, Chapter 6), and work is currently being undertaken on ICT skills and employment issues (www.oecd.org/sti/ICT-employment), and ICT-related offshoring (www.oecd.org/sti/offshoring), both of which address various aspects of digital divide access and policies. The OECD's Working Party on Indicators for the Information Society has agreed on a number of statistical standards for measuring ICT. These standards, along with information on other efforts to measure the information society, have been brought together in the *Guide to Measuring the Information Society* (2005).

[3] CISP was formerly called TISP until March 2006.

### *I. Bridging the Digital Divide: Financing*

The Development Assistance Committee (DAC) is the channel through which donors coordinate, establish best practices, and collectively quantify their development programs. The OECD DAC *Report to the UN Task Force on Financial Mechanisms for ICT for Development (TFFM), "Financing ICTs for Development - Efforts of DAC Members"* (2005), reviewed trends of official development assistance (ODA) with regards to ICT. Building on previous OECD work "Donor ICT Strategies Matrix" (www.oecd.org/dac/ict), it provides policy-oriented analysis of donor support for ICT for development, with particular attention to recent trends in bilateral Official Development Assistance (ODA) commitments for ICT infrastructure, as well as other donor ICT assistance.

### *J. Rules for e-commerce, e-business and consumer protection.*

The OECD has worked on public policy issues that bear on Internet in the course of the work of the Consumer Policy Committee on electronic commerce and consumer protection (www.oecd.org/sti/consumer-policy) and of the OECD Committee on Fiscal Affairs in the course of its work on electronic commerce and taxation. Guidelines include the *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* (2003) and the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2003). OECD analytical work on e-business is summarised in the *Information Technology Outlook 2004*, Chapter 3, which drew conclusions on the uptake and impacts of e-business.