



## **STATEMENT ON INFORMATION SECURITY**

June 2005

### **Introduction**

Information technology has changed the way we do business, and is present in every aspect of the economy -- from banking and finance, transportation and utilities, to food production and distribution, government, and nearly everything else of importance to economic and physical well being. In an automation-reliant society, there is no real physical or economic security without information security. This reality is becoming ever more stark every day, as the global information infrastructure – and the physical infrastructures it supports, comes under attack from hackers and cyber criminals.

Information technology is ubiquitous – that is, computers, networks and software operating everywhere at once – and thus so are vulnerabilities. One challenge is the prevalence of criminal cyber attacks: computer viruses and other malicious code damage or destroy files and data; network intruders steal secrets or other sensitive information; distributed denial of service (DDOS) attacks restrict or eliminate access to the Internet. And, as more sensitive and classified information is made available to more and more users, the insider threat will increase exponentially, making it possible for trusted insiders to engage in criminal activity, including terrorism and economic espionage.

But information technology is not just vulnerabilities and targets, but also offers potent tools for protecting against and responding to attacks, analyzing them and mitigating their damage.

Private industry owns and operates the vast majority of the world's information infrastructure. Protecting global cyber assets is the job of the private sector and the public sector working in partnership as appropriate to secure cyber assets.

In both the public and private sectors, information security challenges must be met with a combination of factors, namely: People, Processes and Technology. Individuals must be vigilant in maintaining the security processes laid out by organizations; organizations must implement and enforce security processes and procedures; and business and government must use multiple layers of security technology to deter threats. All three are necessary to minimize risk.

Technology is ever-changing; business models and processes – and the information systems that support them -- are widely varied; and human interaction with those technologies and processes that provide security is complex and subject to error. But information security is indeed everyone's business, and WITSA encourages a strong public private partnership to catalyze those synergies. Solutions developed collaboratively by industry and public policy makers can help minimize the threat of attack and ensure that our systems remain protected from a new brand of criminal – the cyber criminal.

Without concerted attention to cyber security – in the form of investment, awareness and training, research, information sharing, and other activities – the world’s information will continue to come under ever more sophisticated attack, with costly and potentially catastrophic impact.

## **The World Information Technology and Services Alliance (WITSA)**

The World Information Technology and Services Alliance (WITSA) is a global alliance of national and regional information technology (IT) industry associations from 67 economies around the world. WITSA members represent over 90 percent of the world IT market. As the global voice of the IT industry, WITSA is dedicated to:

- advocating policies that advance the industry’s growth and development;
- facilitating international trade and investment in IT products and services;
- strengthening WITSA’s national industry associations through the sharing of knowledge, experience, and critical information;
- providing members with a vast network of contacts in nearly every geographic region of the world; and
- hosting the World Congress on IT, the premier industry sponsored global IT event.

Founded in 1978 and originally known as the World Computing Services Industry Association, WITSA has increasingly assumed an active advocacy role in international public policy issues affecting the creation of a robust global information infrastructure, including: **increasing competition** through open markets and regulatory reform; protecting **intellectual property**; encouraging cross-industry and government cooperation to enhance **information security**; bridging the education and **skills gap**; **reducing tariff and non-tariff trade barriers** to IT goods and services; and safeguarding the viability and continued growth of the **Internet** and **electronic commerce**.

WITSA has an impact on the global IT environment. It strengthens the industry at large by promoting a level playing field and by voicing the concerns of the international IT community in multilateral organizations, including the World Trade Organization (WTO), the Organization for Economic Cooperation and Development (OECD), the G-8 and other international fora where policies affecting industry interests are developed. More information on WITSA can be found online at <http://www.witsa.org>.

## **International Efforts**

Due to the global nature of the Internet and communications, failure to protect critical information systems and infrastructure at the national, local or even individual level can have global implications. In a networked world, information security is as strong as its weakest link. Countering hacking, allowing strong encryption software, providing mechanisms to deal with viruses, and protecting the privacy of Internet users are all priorities that need to be addressed globally. It is of vital importance that governments and international organizations concerned work closely together and cooperate fully with the private sector.

WITSA has been active in promoting public-private sector cooperation in order to raise awareness and suggest policies and practices that provide greater security for information systems, including convening a Global Information Security Summit in 2000, collaborating on a Global Security Project, issuing statements on cyber crime, and developing a framework for information security. (All materials can be found on the WITSA website – [www.witsa.org](http://www.witsa.org).)

## **Information Security Discussions at the OECD and APEC**

Two international organizations -- the Organization for Economic Cooperation and Development (OECD) and the Asia Pacific Economic Cooperation forum (APEC) – have been actively discussing information security issues. In particular:

### **OECD**

The 1992 OECD Guidelines for the Security of Information Systems were updated to reflect network technologies, typified by the Internet, and changing business practices, including electronic commerce, that have transformed the economic and social importance of information and communication systems since the security guidelines were adopted. The Guidelines offer non-binding recommendations urging governments and industry to cooperate to create an international framework for security of information systems, and encourage industry self-regulatory measures. They call for the joint private and public sector development of regional and national measures, practices and procedures that are simple and compatible with those of other parties that comply with the Guidelines, so as to avoid conflicts and obstacles. These guidelines were complemented in 2003 with the “Information Security Assurance for Executives”, which is intended to give business executives a checklist for information security governance within the enterprise as a way to build a culture of security.

The OECD also has launched an Anti-Spam “Toolkit” as the first step in a broader initiative to help policy makers, regulators and industry restore trust in the Internet and e-mail.

### **APEC**

Within APEC, member economies have combined their efforts to combat threats under the APEC Cybersecurity Strategy, which includes a package of measures to protect business and consumers from Cybercrime, and to strengthen consumer trust in the use of e-commerce. One notable initiative is the development of key public infrastructure guidelines to facilitate cross-jurisdictional e-commerce.

Economies are currently implementing and enacting cybersecurity laws, consistent with the UN General Assembly Resolution 55/63 (2000) and the [Council of Europe?] Convention on Cybercrime (2001). The TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project will support institutions to implement new laws.

Economies are also working together to implement Computer Emergency Response Teams (CERTs) as an early warning defense system against cyber attacks. Training is being provided to a number of economies, and guidelines have been developed for establishing and operating CERTs. The protection of small and medium enterprises is a priority under this strategy. Practical tools to protect small businesses - as well as home users - from attacks and spreading viruses, have been developed, including advice on how to use the internet securely, safety issues relating to wireless technologies and safe e-mail exchanges.

### **Suggested Principles**

In developing industry positions on global Information security issues, WITSA suggests an initial list of general principles that should guide the development of future policy.

## **Joint Principles**

- The Internet and electronic commerce are inherently global in nature; therefore, information security will require collaboration among international bodies and a recognition by government of the challenges faced by industry in these areas.
- Industry and government share an interest in the proliferation of a free and open Internet, electronic commerce, other value-added networks, and an efficient, effective information infrastructure generally.
- Positive interaction between government and industry is essential. Among issues that will require on-going communication and assessment is the need to balance an individual's right to privacy with national security concerns.
- Emergency response organizations must gain sufficient situational awareness and disaster recovery expertise to minimize the effect of catastrophic events on the information infrastructure.

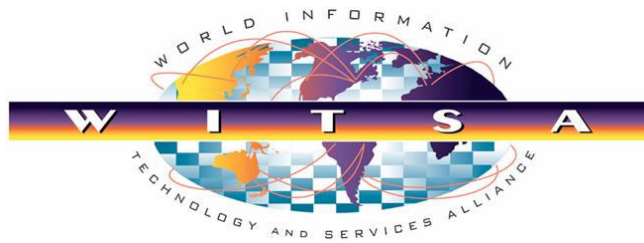
## **Government Principles**

- The assurance of national information infrastructure must be based on the minimum amount of government (national, state/province, and local) regulation as is feasible.
- The cost of protecting national information infrastructure must be kept at a level commensurate with the threat and the consequences of attack.
- Governments must work together internationally to coordinate their own Information security and critical infrastructure assurance programs and activities.
- Where corrective information security action is required to protect the public good, government must identify such instances and create appropriate research, development and funding mechanisms
- In creating and maintaining the information infrastructure and its associated tools and technologies, industry must be provided safe harbor assurances when it has made reasonable efforts and its works viewed as incidental to losses caused by criminal or malicious misbehavior or natural disasters.
- Distinctions must be made among cyber-mischief, cyber-crime and cyber-war to clarify jurisdictional issues and determine appropriate responses. The adequacy of current laws to prevent these threats must be reviewed.
- Existing laws must be adapted as necessary to allow appropriate levels of information sharing among companies, and between the private sector and government.
- Current policy in areas such as the tax credits for research, software encryption, workforce training and long-term government research and development funding must be reviewed in light of common information security goals and objectives.

- Law enforcement agencies on a global basis must gain sufficient cyber-crime expertise to combat specific threats and to investigate specific criminal acts. Also, legal statutes must be updated since in some countries cyber crime is a novelty unrecognized by criminal statutes while the possibility of such crimes being committed is real.

## **Industry Principles**

- Industry owns and operates most of the world's information infrastructures, so should have primary responsibility for information security requirements, design and implementation.
- Industry will be guided by business continuity considerations to protect itself against physical and cyber-attack as the threats to the information infrastructure grow.
- Industry should cooperate both internally and with government in reporting and exchanging non-proprietary information concerning threats, attacks and protective measures. Coordination among principals must facilitate creation of early warning systems.
- Make security a top priority, and put security at the heart of the design process, and where possible, use government, industry and international standards.
- Work with home users, small businesses and large enterprises (including government agencies and educational institutions) in a continual process of improving the security, maintenance and reliability of products that maximize users' productivity.
- Continue to improve the engineering, development, testing and training processes and methods that reduce defects in systems specification, design, implementation and remediation (patching). Partner with government and academia to develop automated tools for evaluating software quality and security.
- Identify, adopt, train and deploy information security best practices with clearly assigned cyber security roles and responsibilities for all employees and organizational leadership.



## The World Information Technology and Services Alliance (WITSA)

<b>Argentina</b>	Cámara de Empresas de Software y Servicios Informáticos (CESSI) URL: <a href="http://www.cessi.org.ar/">http://www.cessi.org.ar/</a> E-mail: <a href="mailto:camara@cessi.org.ar">camara@cessi.org.ar</a>
<b>Armenia</b>	Armenian Union of Information Technology Enterprises (UITE) URL: <a href="http://www.uite.org/">http://www.uite.org/</a> E-mail: <a href="mailto:uite@arminco.com">uite@arminco.com</a>
<b>Australia</b>	Australian Information Industry Association (AIIA) URL: <a href="http://www.aiia.com.au/">http://www.aiia.com.au/</a> E-mail: <a href="mailto:aiia@aiia.com.au">aiia@aiia.com.au</a>
<b>Bangladesh</b>	Bangladesh Computer Samity (BCS) URL: <a href="http://www.bcs-bd.org/">http://www.bcs-bd.org/</a> E-mail: <a href="mailto:samity@dhaka.agni.com">samity@dhaka.agni.com</a>
<b>Benin</b>	AP.TIC Benin – The Professionals of Information and Communication Technology Association URL: <a href="http://www.apticbenin.org">http://www.apticbenin.org</a> E-mail: <a href="mailto:contact@apticbenin.org">contact@apticbenin.org</a>
<b>Brazil</b>	Sociedade de Usuários de Informática e Telecomunicações - Sao Paulo (Sucesu-SP) URL: <a href="http://www.sucesusp.org.br">http://www.sucesusp.org.br</a> E-mail: <a href="mailto:sucesusp@sucesus.org.br">sucesus@sucesus.org.br</a>
<b>Bulgaria</b>	Bulgarian Association of Information Technologies (BAIT) URL: <a href="http://www.bait.bg/">http://www.bait.bg/</a> E-mail: <a href="mailto:bait@spnet.net">bait@spnet.net</a>
<b>Canada</b>	Information Technology Association of Canada (ITAC) URL: <a href="http://www.itac.ca/">http://www.itac.ca/</a> E-mail: <a href="mailto:info@itac.ca">info@itac.ca</a>
<b>Chinese Taipei</b>	Information Service Industry Association of Chinese Taipei (CISA) URL: <a href="http://www.cisanet.org.tw/">http://www.cisanet.org.tw/</a> E-mail: <a href="mailto:cisa@mail.cisanet.org.tw">cisa@mail.cisanet.org.tw</a>
<b>Colombia</b>	Colombian Software Industry Federation (FEDESOFTE) URL: <a href="http://www.fedesoft.org">www.fedesoft.org</a> E-mail: <a href="mailto:proyectos@cati.org.co">proyectos@cati.org.co</a>
<b>Costa Rica</b>	Costa Rican Chamber of Information and Communication Technologies (Camtic) URL: <a href="http://www.camtic.org/">http://www.camtic.org/</a> E-mail: <a href="mailto:fcartin@camtic.org">fcartin@camtic.org</a>
<b>Czech Republic</b>	Association for Consulting to Business (Asociace Pro Poradenství v Podnikání - APP) URL: <a href="http://www.asocpor.cz/">http://www.asocpor.cz/</a> E-mail <a href="mailto:asocpor@asocpor.cz">asocpor@asocpor.cz</a>
<b>Ecuador</b>	Association Ecuatoriana de Tecnología de Información y Servicios (AETIS) URL: <a href="http://www.aetis.org.ec">http://www.aetis.org.ec</a> E-mail: <a href="mailto:aetis@usa.net">aetis@usa.net</a>
<b>Egypt</b>	Egyptian Information Technology, Electronics and Software Alliance (EITESAL) URL: <a href="http://www.eitesal.org">http://www.eitesal.org</a> E-mail: <a href="mailto:moh.fouad@eitesal.com">moh.fouad@eitesal.com</a>
<b>Finland</b>	Federation of the Finnish Information Industries (TIETOALAT) URL: <a href="http://www.finnishinformationindustries.net">http://www.finnishinformationindustries.net</a> E-mail: <a href="mailto:info@tietoalojenliitto.fi">info@tietoalojenliitto.fi</a>
<b>France</b>	Syntec Informatique URL: <a href="http://www.syntec-informatique.fr/">http://www.syntec-informatique.fr/</a> E-mail: <a href="mailto:jpeybert@syntec-informatique.fr">jpeybert@syntec-informatique.fr</a>

<b>Greece</b>	Federation of Hellenic Information Technology and Communications Enterprises (SEPE) URL: <a href="http://www.sepe.gr">http://www.sepe.gr</a> / E-mail: <a href="mailto:sepe@compulink.gr">sepe@compulink.gr</a>
<b>Hong Kong</b>	Hong Kong Information Technology Federation (HKITF) URL: <a href="http://www.hkitf.org.hk">http://www.hkitf.org.hk</a> E-mail: <a href="mailto:mok@hknet.com">mok@hknet.com</a>
<b>Hungary</b>	Hungarian Association of IT Companies (IVSZ) URL: <a href="http://www.ivsz.net">http://www.ivsz.net</a> E-mail: <a href="mailto:szekfu@ivsz.hu">szekfu@ivsz.hu</a>
<b>India</b>	National Association of Software and Service Companies (NASSCOM) URL: <a href="http://www.nasscom.org/">http://www.nasscom.org/</a> E-mail: <a href="mailto:nasscom@nasscom.org">nasscom@nasscom.org</a>
<b>Indonesia</b>	ASPILUKI - Indonesian Telematic Software Association URL: <a href="http://www.aspiluki.or.id/">http://www.aspiluki.or.id/</a> E-mail: <a href="mailto:g_rianto@link.net.id">g_rianto@link.net.id</a>
<b>Israel</b>	Israeli Association of Software Houses (IASH) URL: <a href="http://www.iash.org.il/">http://www.iash.org.il/</a> E-mail: <a href="mailto:software@industry.org.il">software@industry.org.il</a>
<b>Italy</b>	Associazione Nazionale Aziende Servizi Informatica e Telematica URL: <a href="http://www.anasin.it/">http://www.anasin.it/</a> E-mail: <a href="mailto:Anasin@anasin.it">Anasin@anasin.it</a>
<b>Japan</b>	Japan Information Technology Services Industry Association (JISA) URL: <a href="http://www.jisa.or.jp/">http://www.jisa.or.jp/</a> E-mail: <a href="mailto:info@jisa.or.jp">info@jisa.or.jp</a>
<b>Jordan</b>	Information Technology Association - Jordan ( <a href="mailto:int@j">int@j</a> ) URL: <a href="http://www.intaj.net/">http://www.intaj.net/</a> E-mail: <a href="mailto:info@intaj.net">info@intaj.net</a>
<b>Kenya</b>	Computer Society of Kenya (CSK) URL: <a href="http://www.csk-online.org">http://www.csk-online.org</a> ; E-mail: <a href="mailto:charlesnduati2002@yahoo.co.uk">charlesnduati2002@yahoo.co.uk</a>
<b>Lebanon</b>	Professional Computer Association of Lebanon (PCA) URL: <a href="http://www.pca.org.lb/">http://www.pca.org.lb/</a> E-mail: <a href="mailto:Info@pca.org.lb">Info@pca.org.lb</a>
<b>Lithuania</b>	Association of the information technology, telecommunications and office equipment companies of Lithuania (INFOBALT) <a href="http://www.infobalt.lt/">http://www.infobalt.lt/</a> E-mail: <a href="mailto:office@infobalt.lt">office@infobalt.lt</a>
<b>Malaysia</b>	Association of the Computer And Multimedia Industry Malaysia (PIKOM) URL: <a href="http://www.pikom.org.my">http://www.pikom.org.my</a> E-mail: <a href="mailto:info@pikom.org.my">info@pikom.org.my</a>
<b>Mexico</b>	Asociación Mexicana de la Industria de Tecnologías de Información (AMITI) URL: <a href="http://www.amiti.org.mx/">http://www.amiti.org.mx/</a> E-mail: <a href="mailto:amiti@amiti.org.mx">amiti@amiti.org.mx</a>
<b>Mongolia</b>	Mongolian National Information Technology Association; <a href="mailto:badarch@magicnet.mn">badarch@magicnet.mn</a>
<b>Morocco</b>	l'Association des Professionnels des Technologies de l'Information (APEBI); <a href="http://www.apebi.org.ma/">http://www.apebi.org.ma/</a> E-mail: <a href="mailto:apebi@apebi.org.ma">apebi@apebi.org.ma</a>
<b>Nepal</b>	Computer Association of Nepal (CAN) / <a href="http://www.can.org.np/">http://www.can.org.np/</a> / <a href="mailto:info@can.mos.com.np">info@can.mos.com.np</a>
<b>Netherlands</b>	Federation of Dutch Branch Associations in Information Technology (Federatie Nederlandse IT - FENIT) URL: <a href="http://www.fenit.nl/">http://www.fenit.nl/</a> E-mail: <a href="mailto:bureau@fenit.nl">bureau@fenit.nl</a>
<b>Netherlands Antilles</b>	Curacao Information & Communication Association (CICA) URL: <a href="http://www.cica.an/">http://www.cica.an;</a> E-mail: <a href="mailto:info@cica.an">info@cica.an</a>
<b>New Zealand</b>	Information Technology Association of New Zealand (ITANZ) URL: <a href="http://www.itanz.org.nz/">http://www.itanz.org.nz/</a> E-mail: <a href="mailto:info@itanz.org.nz">info@itanz.org.nz</a>
<b>Northern Ireland</b>	Momentum - The Northern Ireland ICT Federation URL: <a href="http://www.momentumni.org">http://www.momentumni.org</a> E-mail: <a href="mailto:billy@momentumni.org">billy@momentumni.org</a>
<b>Norway</b>	ICT Norway (IKT Norge) / <a href="http://www.ikt-norge.no/">http://www.ikt-norge.no/</a> E-mail: <a href="mailto:bt@ikt-norge.no">bt@ikt-norge.no</a>

<b>Palestine</b>	Palestinian IT Association (PITA) URL: <a href="http://www.pita-palestine.org/">http://www.pita-palestine.org/</a> E-mail: <a href="mailto:info@pita-palestine.org">info@pita-palestine.org</a>
<b>Panama</b>	Asociación Panameña de Software (APS) <a href="http://www.aps.org.pa/">http://www.aps.org.pa/</a> / <a href="mailto:aps@arango.com">aps@arango.com</a>
<b>Philippines</b>	Information Technology Association of the Philippines (ITAP) URL: <a href="http://www.itaphil.org/">http://www.itaphil.org/</a> E-mail: <a href="mailto:cvparlade@pablaw.com.ph">cvparlade@pablaw.com.ph</a>
<b>Poland</b>	Polish Chamber of Information Technology and Telecommunications (Polska Izba Informatyki i Telekomunikacji - PIIT) / <a href="http://www.piit.org.pl/">http://www.piit.org.pl/</a> Email: <a href="mailto:biuro@piit.org.pl">biuro@piit.org.pl</a>
<b>Portugal</b>	Associação Portuguesa das Empresas de Tecnologias de Informação e Comunicações (APESI) E-mail: <a href="mailto:apesi@treal.pt">apesi@treal.pt</a>
<b>Republic of Korea</b>	Federation of Korean Information Industries (FKII) URL: <a href="http://www.fkii.or.kr/">http://www.fkii.or.kr/</a> E-mail: <a href="mailto:grant@fkii.org">grant@fkii.org</a>
<b>Republic of Macedonia</b>	Macedonian Association of Information Technology (MASIT) URL: <a href="http://www.masit.org.mk">http://www.masit.org.mk</a> E-mail: <a href="mailto:contact@masit.org.mk">contact@masit.org.mk</a>
<b>Romania</b>	Association for Information Technology and Communications of Romania (ATIC) URL: <a href="http://www.atic.org.ro">http://www.atic.org.ro</a> E-mail: <a href="mailto:atic@softnet.ro">atic@softnet.ro</a>
<b>Russia</b>	Russian Information & Computer Technologies Industry Association (APKIT) URL: <a href="http://www.apkit.ru/">http://www.apkit.ru/</a> E-mail: <a href="mailto:info@apkit.ru">info@apkit.ru</a>
<b>Senegal</b>	Senegalese Information Technology Association (SIT'SA) <a href="http://www.sitsa.sn/">www.sitsa.sn/</a> / <a href="mailto:sitsa@sitsa.sn">sitsa@sitsa.sn</a>
<b>Singapore</b>	Singapore infocomm Technology Federation (SiTF) <a href="http://www.sitf.org.sg/">http://www.sitf.org.sg/</a> / <a href="mailto:sitf@sitf.org.sg">sitf@sitf.org.sg</a>
<b>South Africa</b>	Information Industry South Africa (IISA) URL: <a href="http://www.informationindustry.org.za/">http://www.informationindustry.org.za/</a> E-mail: <a href="mailto:info@informationindustry.org.za">info@informationindustry.org.za</a>
<b>Spain</b>	Spanish Association of Electronics, Information Technology and Telecommunications Companies (AETIC) URL: <a href="http://www.aetic.es/">http://www.aetic.es/</a> E-mail: <a href="mailto:aetic@aetic.es">aetic@aetic.es</a>
<b>Sri Lanka</b>	Sri Lanka Information and Communications Technology Association (SLICTA) E-mail: <a href="mailto:sg@searcc.org">sg@searcc.org</a> ; <a href="http://www.slicta.lk/">http://www.slicta.lk/</a>
<b>Sweden</b>	The Association of the Swedish IT and Telecom Industry (IT-Företagen) URL: <a href="http://www.itforetagen.se/">http://www.itforetagen.se/</a> E-mail: <a href="mailto:info@itforetagen.se">info@itforetagen.se</a>
<b>Syria</b>	Syrian Computer Society (SCS); URL: <a href="http://www.scs.org.sy">www.scs.org.sy</a> , E-mail: <a href="mailto:sec@scs-net.org">sec@scs-net.org</a>
<b>Tanzania</b>	Tanzania Information and Communication Technologies Association (TICTA)
<b>Thailand</b>	The Association of Thai Computer Industry (ATCI) URL: <a href="http://www.atci.or.th/">http://www.atci.or.th/</a> E-mail: <a href="mailto:Info@ATCI.or.th">Info@ATCI.or.th</a>
<b>Trinidad &amp; Tobago</b>	The Information Technology Professional Society of Trinidad and Tobago (ITPS); URL: <a href="http://www.itps.org/">http://www.itps.org/</a> ; E-mail: <a href="mailto:itps@itps.org">itps@itps.org</a>
<b>Tunisia</b>	Tunisian IT Chamber (National Chamber of Information Technology Engineering and Services Companies – CNS-SSII); URL: <a href="http://www.ssii.org.tn/">http://www.ssii.org.tn/</a> ; E-mail: <a href="mailto:info@ssii.org.tn">info@ssii.org.tn</a>
<b>Turkey</b>	Turkish IT Services Association (TUBISAD) URL: <a href="http://www.tubisad.org.tr">http://www.tubisad.org.tr</a> E-mail: <a href="mailto:tubisad@tubisad.org.tr">tubisad@tubisad.org.tr</a>
<b>Uganda</b>	The Private-Sector ICT Association of Uganda (PICTA) URL: <a href="http://www.picta.or.ug/">http://www.picta.or.ug/</a> E-mail: <a href="mailto:info@picta.or.ug">info@picta.or.ug</a>

<b>Ukraine</b>	Association "Information Technologies of Ukraine" (IT Ukraine); URL: <a href="http://www.itukraine.org.ua/">http://www.itukraine.org.ua/</a> ; E-mail: <a href="mailto:nroyenko@miratech-software.com">nroyenko@miratech-software.com</a>
<b>United Kingdom</b>	The Information Technology, Telecommunications and Electronics Association (Intellect) URL: <a href="http://www.intellectuk.org">http://www.intellectuk.org</a> E-mail: <a href="mailto:info@intellectuk.org">info@intellectuk.org</a>
<b>United States</b>	Information Technology Association of America (ITAA) URL: <a href="http://www.ita.org/">http://www.ita.org/</a> E-mail: <a href="mailto:jmcwilliams@ita.org">jmcwilliams@ita.org</a>
<b>Uruguay</b>	Uruguayan Chamber of Information Technology (CUTI) URL: <a href="http://www.cuti.org.uy/">http://www.cuti.org.uy/</a> E-mail: <a href="mailto:info@cuti.org.uy">info@cuti.org.uy</a>
<b>Venezuela</b>	CAVEDATOS - Venezuelan Chamber of IT Companies URL: <a href="http://www.cavedatos.org.ve/">http://www.cavedatos.org.ve/</a> E-mail: <a href="mailto:cavedato@telcel.net.ve">cavedato@telcel.net.ve</a>
<b>Vietnam</b>	VINASA - Vietnam Software Association URL: <a href="http://www.vinasa.org">http://www.vinasa.org</a> E-mail: <a href="mailto:office@vinasa.org">office@vinasa.org</a>
<b>Zimbabwe</b>	Computer Suppliers' Association of Zimbabwe (COMSA) <a href="http://www.comsa.org.zw/">http://www.comsa.org.zw/</a> / <a href="mailto:comsa@csz.icon.co.zw">comsa@csz.icon.co.zw</a>