



**WITSA Resolution
on
Cyber Security
in
Hyderabad, India
December 2, 2008**

The World Information Technology and Services Alliance (WITSA) industry recognizes that the ubiquitous nature of the Internet and information networks across the globe provides for greater productivity, efficiency, and innovation than ever before, but it also provides for greater vulnerabilities to attack, manipulation, and theft.

As such, we believe that industry, government, and [individuals/civil society] around the world should take steps to increase their cyber security posture.

In addition, given that networks are global and cyberspace is borderless, industry, government, and [individuals/civil society] around the world need to find ways to collaborate and share information with each other both at home and abroad.

The WITSA also recognizes that the industry moves very quickly with new products and services introduced at a rapid rate. At the same time, the threat environment also evolves very quickly as new actors and new threat vectors emerge. Combined, these two dynamics make for a fluid risk environment. As such, we believe that there is no one solution that can address all the issues we face – either today or tomorrow. As the environment evolves, so do our needs, and we need to be agile enough to address those changing needs over time.

Countries and multilateral organizations are increasingly embracing cyber security policy and practices, which is a positive development as that provides more opportunity for collaboration and progress for global cyber security efforts. We appreciate the work of organizations such as: the Organisation for Economic Cooperation and Development (OECD), the Asia Pacific Economic Cooperation (APEC), the United Nations (UN), the International Telecommunications Union (ITU), the Organization for American States (OAS), the Council of Europe (COE), the European Union (EU), the North Atlantic Treaty Organization (NATO), the Group of 8 (G-8), l'Organisation internationale de la

Francophonie, l'Union Africaine and other regional groups on their various efforts to address cyber security and cyber crime. However, we believe that multilateral efforts need to reflect the flexibility needed to respond to the evolving environment, and to complement, rather than duplicate the efforts of related organizations.

The WITSA recognizes the respective roles of industry and government in providing for protective measures and cyber security efforts. Industry owns and operates the majority of our critical information infrastructure globally, while government has a duty to ensure the security of its own information networks and services to its citizenry. We believe that partnership is crucial to managing those roles and responsibilities and to ensuring productive synergies for progress.

Given these overarching tenets of cyber security in the international context, WITSA sets forth the following global cyber security principles:

WITSA CYBER SECURITY PRINCIPLES

- **The Internet and information networks are global in nature; therefore, cyber security requires international collaboration through bilateral and plurilateral efforts and through multilateral organizations that enables flexibility, innovation, and private sector leadership;**
- **Information networks are ubiquitous and used by so many for their communications needs and operations; therefore, governments and organizations should address cyber security as a fundamental and cross-cutting issue;**
- **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; therefore, cyber security efforts should be undertaken in a way that does not inhibit innovation;**
- **There is no static or one-size fits all solution to “perfect” cyber security; therefore, cyber security efforts should be part of a dynamic, risk management-based approach to protection, detection, and mitigation;**
- **No on entity can solve cyber security issues alone; therefore, government and industry must find ways to collaborate, share information and analysis, and identify appropriate roles and responsibilities for protection, detection, and mitigation efforts both domestically and internationally, including adapting existing laws, if necessary;**
- **Our global networks provide critical communications and operational services to government, industry, and individuals around the world; therefore, in order to further assure those services, cyber security should be considered as a fundamental and foundational tenet in all efforts such as the development of government services, company product design, and consumer behavior;**
- **Companies and individuals have been increasingly targeted by cyber criminals from all over the world; therefore, law enforcement agencies must have the ability to collaborate and cooperate on a global basis, and criminal statutes must incorporate cyber crime so that those criminals can be prosecuted.**