



Office of the President of the Philippines  
COMMISSION ON INFORMATION AND COMMUNICATIONS TECHNOLOGY

**IT SECURITY FORUM ON  
“MAPPING THE FUTURE OF INFORMATION SECURITY”**

29 July 2008, 9:10-9:30 AM  
Grand Ballroom, Hotel Intercontinental, Makati City

---

Keynote Address

**“Guidelines for Implementing Information Security Programs and Projects”**

by **SECRETARY RAY ANTHONY ROXAS-CHUA III**

Commission on Information and Communications Technology

I would like to congratulate the Information Systems Security Society of the Philippines (ISSSP) for orchestrating this “*Forum on Mapping the Future of Information Security.*” We are honored to have been invited to speak on the topic “Guidelines for Implementing Information Security Programs and Projects,” which is one of the most important initiatives that the CICT is pursuing.

In today’s knowledge economy, organizations do not only concern themselves with the management of human resources, machineries, production plants, or product designs but they also consider information as a very important asset. Whatever form it may take—printed on paper, stored electronically, channeled through post or electronic means, depicted on films or spoken in conversation—information shapes the world’s business, governance, education and social landscapes. Breakthroughs in telecommunications and the unparalleled growth of the World Wide Web are said to have resulted in three trends.

First, the Internet has transformed the conduct of business and how human exchanges occur thereby producing interconnected business and social environments.

Second, interconnectivity puts information at higher risk of being exposed to cybersecurity threats such as hacking, identity theft, spamming, phishing, denial-of-service attacks, malware, malicious code, computer-assisted fraud, industrial/military espionage and sabotage, as well as natural phenomena like fires, floods, and earthquakes.

Lastly, the vitality of information calls for effective management and protection against cybersecurity threats to ensure continuous business existence, multiply business opportunities, counter business risks, and maximize the return on investment.

With the abovementioned trends also evolved the field of Information Security. In its basic definition, Information Security means the preservation of (1) confidentiality (information is accessible only to those who have authorized access to it), (2) integrity (safeguarding the accuracy and completeness of information and processing methods) and (3) availability of information (authorized users have timely access to information and associated assets).

Information security is a primary concern of the CICT being the ICT policy-making entity of the government. The country's booming ICT industry and Philippine government's commitment to widespread ICT adoption have made the field an important consideration in CICT's policy-making efforts. The CICT's information security strategies are incorporated in two frameworks.

The National Cyberspace Security Plan 2005 stipulates that "*the primary task of creating a conducive environment for the protection of critical cyberspace infrastructures still falls under government responsibility*". In compliance with this direction, the government, through the CICT, shall work for four significant goals:

- (1) Assure the continuous operation of our nation's critical cyberspace infrastructure;
- (2) Implement capacity building measures to enhance our ability to respond to threats before, during and after attacks;
- (3) Practice effective law enforcement and administration of justice; and
- (4) Enhance society's cyberspace security consciousness.

Further, the 2006-2010 Philippine Strategic ICT Roadmap affirms that the CICT's chief role in ICT development is to foster an enabling policy, legal and regulatory environment that levels the playing field and empowers the private sector to lead. The CICT is also mandated to provide a safe and trustworthy online environment as a critical component of the Philippine Information Society.

The CICT encourages effective information security measures in support of its two strategic priorities which are the Cyber Corridor and E-Government. The Cyber Corridor seeks to develop ICT investment hubs outside Metro Manila and disperse economic opportunities to the regions. Information security will help ICT service providers in the Cyber Corridor to gain a competitive edge, maintain profitability, and comply with legal and business ethics. In E-Government, information security will help protect critical digital infrastructures, enable implementation of e-government and e-commerce initiatives and reduce relevant risks.

Meanwhile, the private sector also assumes a pivotal role in the realization of the national ICT agenda. The chapter on Digital Infrastructure in the 2004-2010 Medium-Term Philippine Development Plan (MTPDP) clearly states that "*in realization of the full potentials of ICT as a tool for knowledge creation and diffusion, the private sector will lead the deployment and expansion of digital infrastructure and the convergence of telecommunications technologies while implementing security measures to protect their integrity.*"

In closing, I would like to encourage my fellow government workers and our private sector partners present here to embody the principle of "shared responsibility" which requires the private and public sectors to coordinate strategies and share resources and expertise in the effective management and protection of our country's online environment.

Thank you very much and I wish everyone a fruitful forum.