TELECOMMUNICATIONS REGULATORY AUTHORITY

بسم الله الرحمن الرحيم

Your Excellencies, Ladies and Gentlemen,

Lionel Giles once said: *"Everybody can see superficially how a battle is won; what they cannot see are the long series of plans and combinations which have preceded the battle"*

During the past decade, the UAE has become one of the most critical business hubs in the region. Thus, the need arises to safeguard the critical information and communication technology infrastructure residing under the government, business, and education sectors.

Today we live in a new technological era, where everyday and every moment spill out a new array of cyber security threats and risks that may affect the businesses adversely. An attacker can create an enormous amount of damage with a quite small investment, while businesses spend a great deal to counteract the threats.

Hence, rather than only reacting, businesses today need to implement a proactive, structured and business-focused approach to information security in their organizations.

This year, the UAE counteracted many attacks, mainly website defacement, phishing attacks, and many others. These attacks caused immense damage to the businesses, affecting the core principles of information security that are based on confidentiality, integrity and availability.

Last month, however, an Internet Fraud Ring was crushed, where the fraudsters have setup fictitious and non-existent websites claiming to offer financial services to the Internet customers. Such a successful counteractive action that crushed

the fraudsters, institutes readiness to face cyber security breaches, as well as concerns to further develop emergency security strategy to safeguard the cyber space from saboteurs.

For such vital reasons, the Telecommunications Regulatory Authority (TRA) of the UAE has introduced a new initiative to establish the United Arab Emirates Computer Emergency Response Team (aeCERT), which will constitute a cyber security coordination center in the UAE. This initiative will facilitate the detection, prevention and response to the broader set of cyber security incidents on the Internet.

The aeCERT will, by no doubt, enhance the cyber security law and assist in the creation of new laws; will enhance information security awareness across the UAE; will build national expertise in information security, incident management and computer forensics; will provide a central trusted point of contact for cyber security incident reporting in the UAE; will establish a national center to disseminate information about threats, vulnerabilities and cyber security incidents; will foster the establishment of and provide assistance to sector-based Computer Security Incidents Research Teams (CSIRTs); will coordinate with domestic and international CSIRTs and related organizations; and will become an active member of recognized security organizations and forums. I, however, have faith that aeCERT will succeed to present a proactive and structured approach to deter the future coming cyber security incidents.

Still, I forecast the success of this conference, due to its program and participants that include with 20 network security specialists and researchers, 4-tracks of hands on technical training sessions, network assessment and latest attack methods, fundamental defense methodologies, close look at the latest computer and network security technologies, advanced computer and network security topics, 2-days of deep knowledge papers and presentations, and live hacking competition.

Finally, I welcome you to the United Arab Emirates, and wish you all an informative and successful conference.

**Thank you!**