National Electric Power Regulatory Authority
Islamic Republic of Pakistan

NEPRA Tower, Ataturk Avenue (East) G-5/1, Islamabad
Ph: +92-51-2013200, Fax: +92-51-9210215, +92-51-2600050
Web: www.nepra.org.pk, E-mail: Office@nepra.org.pk

Islamabad, February 19, 2021

PRESS RELEASE

Subject: **First-ever Webinar on Industrial Cyber Security Hosted**

NEPRA today hosted Pakistan's first-ever webinar on Industrial Cyber Security with title "The Modern Threat Landscape on Industrial Control Systems – Statistics and Examples" at NEPRA Tower with an aim to create awareness amongst the public and private sector's power entities against the global risks of cyberattacks. The webinar was led and addressed by Chairman NEPRA, Mr. Tauseef H. Farooqi, followed by internationally renowned cybersecurity experts from Russia, Dr. Semen Kort and Dr. Ekaterina Rudina of Kaspersky Industrial Cybersecurity (KICS). The webinar was attended by a large number of Power Sector's Professionals, Trade and Business representatives, journalists and NEPRA's members of the Authority and professionals.

02. The Chairman NEPRA, Mr. Tauseef H. Farooqi in his welcoming address highlighted the importance of the webinar. He remarked that Pakistan like rest of the world is also witnessing multiple cyberattacks and data breaches simultaneously and therefore this global menace needs to be tackled with comprehensive effective measures. He added that Pakistan's power sector Industrial Control Systems are prone to such attacks and therefore a single vulnerability can result in unexpected outages, loss of revenue for industry and even loss of human lives; thus the economy can be easily impacted. He added that NEPRA being the regulator of Power Sector of Pakistan will strive for launching prudent regulations in order to effectively handle such existing and future sophisticated cyberattacks to protect our National Critical Power Assets.

03. Dr. Semen Kert and Dr. Ekaterina Rudina sensitized the participants about various types of Industrial cyberattacks and vulnerabilities, the social engineering attacks, differences in the implementation of cyber security in the systems, Industrial security solutions, remote access, importance of an effective cyber security department, incidents handling and the need for regulations so that the threats are effectively handled.

04. The webinar concluded after detailed Questions & Answers session of the participants with the Chairman and the Speakers.

***** End *****