

## President

SEC/GEN/MA/2021/063

12<sup>th</sup> March 2021

*Hon'ble Minister,*

### **Sub.: Cyber Security threat from Category 1 High Risk Products imported from China**

Critical Infrastructure, especially electricity generation, transmission and distribution (including financial transactions), load despatch systems and network, is highly vulnerable to Cyber threats and Malware -Trojan attacks. This has been duly acknowledged during discussions at various levels with CEA and MOP. The main reason is unstructured implementation of technology and products in recent past, particularly imported from China, which opens gates for cyber attacks. This vulnerability is particularly severe with distribution utilities, which have limited skills on Cyber Security and are largely dependent on their vendors (from China in many cases).

In recent past, there have been cyber attacks in many countries around the world. IEEMA has been strongly advocating for minimising our dependency on Chinese equipment since 2014. Consequent to our raising specific issues of possible threat to our electricity network from China sponsored cyber attacks, a Committee was formed under the CEA, where IEEMA was a member. Copy of the Report of this Committee titled "Cyber Security in Power System" is attached for ready reference.

One element strongly emerging from the report is the need for identifying and isolating the equipment of Chinese origin installed in our electricity network, especially products which are high risk in terms of cyber sensitivity, evaluating their threat potency and examining their replacement. Products which we feel to be "Category 1 High Risk" in terms of cyber sensitivity are Remote Terminal Units, FRTUs, Networking Equipment - Router, Firewall, Communication Module, SCADA Equipment & Software, Ethernet Switch card, Automatic Data Processing Machine/ CPU, PCB Cards, Switches, automation and control products, remote operation and communication systems, and industrial computers.

proud partners in implementation



INDIAN ELECTRICAL EQUIPMENT INDUSTRY  
**MISSION PLAN**  
2012-2022

**Mumbai:**  
501, Kakad Chambers,  
132, Dr. Annie Besant Road, Worli,  
Mumbai 400018, INDIA.  
P: +91 22 2493 0532  
F: +91 22 2493 2705  
E: mumbai@ieema.org

**Bangalore:**  
204, Swiss Complex,  
33, Race Course Road,  
Bangalore 560 001, INDIA.  
P: +91 80 2220 1316 / 1318  
F: +91 80 2220 1317  
E: bangalore@ieema.org

**Kolkata:**  
503A, Oswal Chambers,  
2, Church Lane,  
Kolkata - 700 001, INDIA.  
P: +91 33 6510 7855  
F: +91 33 2213 1326  
E: kolkata@ieema.org



A study of India's import of these Category 1 High Risk products from China during last 7 years reveals a net import of over USD 20,000 million. Table giving details of import of individual products from China is attached; data based on DGCIS statistics.

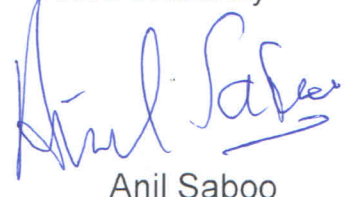
Presence of these high risk items of Chinese origin in the critical area of electrical power system (especially transmission and distribution) network is fraught with danger.

Instances have also started surfacing that Chinese companies are manipulating Indian customers by not supplying the required spares for equipment delivered in the past. Utilities, both at states and central PSUs, have reported that efforts to reach out to the Chinese OEMs, either directly or through the local EPC player involved in installation of those systems, are not yielding any result as the Chinese OEMs are not responding to their calls for spares.

In view of the above, we earnestly request the Government to examine the installed base of such equipment of Chinese origin in our power system (including transmission and distribution) network across all utilities. All central PSUs and Utilities in states, whether Government owned or private, franchises or licensees, should be asked to **identify** such installations within their respective domains, **isolate** all equipment of Chinese origin and **evaluate** their threat potency with a view of their **replacement** with products manufactured indigenously or by manufacturers from friendly countries. This activity deserves top priority, given the seriousness of Cyber Security threats to our electricity network from China sponsored players located across the globe.

*Best Regards*

Yours sincerely

  
Anil Saboo

**Shri R.K. Singh**  
Hon'ble Minister of Power and MNRE  
Government of India  
**Ministry of Power**  
Shram Shakti Bhavan  
**New Delhi - 110001**