from: **SITARA** <chairperson@sitara.org.in>

to: rajkumar.singh19@sansad.nic.in,
Mos-pcm@gov.in,
rksinghmpara@gmail.com

cc: cimoffice <cimoffice@nic.in>,
secy-power@nic.in,
prinsec.pmo@gov.in,
pkmishra.pmo@gov.in,
pksinha.pmo@gov.in,
cabinetsy@nic.in,
office-psa@nic.in,
secy-ipp@nic.in,
Ajay Kumar <ajay@gov.in>,
Dynsasa-nscs@gov.in,
Rajesh Pant <ncsc@gov.in>,
"P.S.Raghavan" <raghavan.ps@gmail.com>,
vijayraghavan@gov.in,
SITARA <India-Sitara@googlegroups.com>,
secy-dot@nic.in

date: Jul 4, 2020, 6:15 PM

subject: Power Ministry's welcome step & Need to remove Chinese from PGCIL networks

mailed-by: sitara.org.in

On Sat, Jul 4, 2020 at 6:15 PM SITARA <chairperson@sitara.org.in> wrote:

To

**Shri Raj Kumar Singh**

Hon’ble Minister of State for Power (Independent Charge)

Ministry of Power

Shram Shakti Bhawan

New delhi-110001

Email: rajkumar.singh19@sansad.nic.in

Saturday, July 4, 2020

Dear Sir,

On behalf of SITARA, the Science, Indigenous Technology & Advanced Research Accelerator, a Trust dedicated to make India a scientifically and technologically advanced Nation, we laud your decision to stop imports of Chinese power equipment. Apart from the clear and grave security risks arising from such imports, we are happy that you also emphasised the need for domestic procurement so that the Indian economy can grow and high-tech, high value jobs can be created at home. We sincerely appreciate your decision which will uphold both National & Economic Security.

In this connection, we also wish to point out that **Chinese ownership of Indian communications networks, particularly those tendered by “Powertel” [of the Power Grid Corporation of India Ltd (PGCIL)], also poses a critical danger to our country**. India’s power-grid is part of its Critical Infrastructure and is particularly vulnerable to remote shut-down by hostile powers. We also hear that the PowerGrid Telecom Network is being used by various Government agencies like NIC, Intelligence Bureau (IB), DRDO, NKN etc., so the security risks to sensitive communications are clear.

**Despite this, we have learnt that PGCIL has once again awarded a sensitive tender** - **Telecom Equipment (DWDM) Package-U under Augmentation of Telecom Backbone and Access Network; Specification No:  CC-CS/842-SR2/TELE-3791/3/G6-**  **to a Chinese company** **– FiberHome.** It may kindly be noted that bids by the Chinese companies FiberHome (reportedly Rs 153 cr) and ZTE (Rs. 211) were significantly below Power Grid’s budgeted estimate of Rs 270 crores and indicated **massive predatory pricing and hidden Chinese State support for *taking over another sensitive Indian Government network.*** PGCIL may not be expected to understand the security risks involved, as the enclosed article suggests, but there is no doubt that we are opening ourselves to enormous security risks by awarding sensitive communications tenders to Chinese companies.

Chinese companies have systematically bid for sensitive Government networks over the past few years. Chinese companies win tenders the world over through *ruthless underbidding* and*other allegedly unethical practices***.** **This is because in a digitized age, China understands the strategic value of control over a country’s ICT networks, which gives it unparalleled power over data flows and physical grids, which can be shut down or sabotaged remotely with full deniability.** **It is not just via insertion of malware and Trojan horses in telecom and networking equipment that can trigger electricity grid failures to cripple economic activity, this can also be achieved through physical control of the networks, which China has been given. So it is China's  physical control over our networks which has to be ended, as other countries are doing around the world.  This is in accordance with their Information Warfare doctrine which is at the core of Chinese military strategy. As you have pointed out, China can indeed shut down our ICT networks remotely.**

We have been requesting Government to apply national security and economic security criteria in tendering procedures, and we are heartened to know that this is being considered. Two of our communications to Hon’ble PM and NSCS are enclosed. **The recent surprise Chinese attack on our steadfast and brave troops has completely vindicated our repeated warnings not to trust equipment from our adversary and develop our own domestic capabilities.**

**We thus hope that the ban on Chinese power equipment imports will also include any Chinese telecom equipment used in PowerGrid’s and Powertel’s network such as in this tender [Telecom Equipment (DWDM) Package-U under Augmentation of    Telecom    Backbone and Access Network; Specification No:  CC-CS/842-SR2/TELE-3791/3/G6]. In fact, the tender itself should be fully disallowable on National Security Grounds.**

**China’s predatory tactics have driven Indian companies out of their own market – India - and weakened our nation as our companies go out of business, rendering us severely import dependent. Hon’ble PM has called for rectifying this vulnerability and your decision is a big step in that direction. We therefore request you to please authorize a thorough security audit of Power Grid’s networks, given the proven hostility demonstrated by China, and removal of Chinese equipment from them. We have learnt that PGCIL has given earlier tenders to Chinese companies and these should also be reviewed.**

**After the cyber-attack on a nuclear power facility and the death of / sacrifice by our soldiers, Government cannot afford to wait anymore to neutralise the gathering risk arising from Chinese physical control of our networks. A whole of Government united approach is required to deal with the Chinese threat.**

With respectful regards,

Smita Purushottam

Ambassador (Retd.) & Chairperson

SITARA



The Science, Indigenous Technology & Advanced Research Accelerator

To

**Shri Raj Kumar Singh**

Hon’ble Minister of State for Power (Independent Charge)

Ministry of Power

Shram Shakti Bhawan

New delhi-110001

Email: rajkumar.singh19@sansad.nic.in

Saturday, July 4, 2020

Dear Sir,

On behalf of SITARA, the Science, Indigenous Technology & Advanced Research Accelerator, a Trust dedicated to make India a scientifically and technologically advanced Nation, we laud your decision to stop imports of Chinese power equipment. Apart from the clear and grave security risks arising from such imports, we are happy that you also emphasised the need for domestic procurement so that the Indian economy can grow and high-tech, high value jobs can be created at home. We sincerely appreciate your decision which will uphold both National & Economic Security.

In this connection, we also wish to point out that **Chinese ownership of Indian communications networks, particularly those tendered by “Powertel” [of the Power Grid Corporation of India Ltd (PGCIL)], also poses a critical danger to our country**. India’s power-grid is part of its Critical Infrastructure and is particularly vulnerable to remote shut-down by hostile powers. We also hear that the PowerGrid Telecom Network is being used by various Government agencies like NIC, Intelligence Bureau (IB), DRDO, NKN etc., so the security risks to sensitive communications are clear.

**Despite this, we have learnt that PGCIL has once again awarded a sensitive tender** - **Telecom Equipment (DWDM) Package-U under Augmentation of Telecom Backbone and Access Network; Specification No: CC-CS/842-SR2/TELE-3791/3/G6-** **to a Chinese company** **– FiberHome.** It may kindly be noted that bids by the Chinese companies FiberHome (reportedly Rs 153 cr) and ZTE (Rs. 211) were significantly below Power Grid’s budgeted estimate of Rs 270 crores and indicated **massive predatory pricing and hidden Chinese State support for *taking over another sensitive Indian Government network.*** PGCIL may not be expected to understand the security risks involved, as the enclosed article suggests, but there is no doubt that we are opening ourselves to enormous security risks by awarding sensitive communications tenders to Chinese companies.

Chinese companies have systematically bid for sensitive Government networks over the past few years. Chinese companies win tenders the world over through *ruthless underbidding* and*other allegedly unethical practices***.** **This is because in a digitized age, China understands the strategic value of control over a country’s ICT networks, which gives it unparalleled power over data flows and physical grids, which can be shut down or sabotaged remotely with full deniability.** **It is not just via insertion of malware and Trojan horses in telecom and networking equipment that can trigger electricity grid failures to cripple economic activity, this can also be achieved through physical control of the networks, which China has been given. So it is China’s physical control over our networks which has to be ended, as other countries are doing around the world.** **This is in accordance with their Information Warfare doctrine which is at the core of Chinese military strategy. As you have pointed out, China can indeed shut down our ICT networks remotely.**

We have been requesting Government to apply national security and economic security criteria in tendering procedures, and we are heartened to know that this is being considered. Two of our communications to Hon’ble PM and NSCS are enclosed. **The recent surprise Chinese attack on our steadfast and brave troops has completely vindicated our repeated warnings not to trust equipment from our adversary and develop our own domestic capabilities.**

**We thus hope that the ban on Chinese power equipment imports will also include any Chinese telecom equipment used in PowerGrid’s and Powertel’s network such as in this tender [Telecom Equipment (DWDM) Package-U under Augmentation of Telecom Backbone and Access Network; Specification No: CC-CS/842-SR2/TELE-3791/3/G6]. In fact, the tender itself should be fully disallowable on National Security Grounds.**

**China’s predatory tactics have driven Indian companies out of their own market – India - and weakened our nation as our companies go out of business, rendering us severely import dependent. Hon’ble PM has called for rectifying this vulnerability and your decision is a big step in that direction. We therefore request you to please authorize a thorough security audit of Power Grid’s networks, given the proven hostility demonstrated by China, and removal of Chinese equipment from them. We have learnt that PGCIL has given earlier tenders to Chinese companies and these should also be reviewed.**

**After the cyber-attack on a nuclear power facility and the death of / sacrifice by our soldiers, Government cannot afford to wait anymore to neutralise the gathering risk arising from Chinese physical control of our networks. A whole of Government united approach is required to deal with the Chinese threat.**

With respectful regards,

Smita Purushottam

Ambassador (Retd.) & Chairperson

SITARA